# TransPortal™ Interlock Monitor

| ASTS USA Part No. |
| --- |
| N37404000<br>SNMP-Based TransPortal |

- Installation
- Operation
- Troubleshooting

Copyright© 2009
Ansaldo STS USA, Inc.

# Proprietary Notice

This document and its contents are the property of Ansaldo STS USA, Inc. (formerly known as Union Switch & Signal Inc., and hereinafter referred to as "ASTS USA"). This document is furnished to you on the following conditions: 1.) That no proprietary or intellectual property right or interest of ASTS USA is given or waived in supplying this document and its contents to you; and, 2.) That this document and its contents are not to be used or treated in any manner inconsistent with the rights of ASTS USA, or to its detriment, and are not to be copied, reproduced, disclosed or transferred to others, or improperly disposed of without the prior written consent of ASTS USA.

# Important Notice

ASTS USA constantly strives to improve our products and keep our customers apprised of changes in technology. Following the recommendations contained in the attached service manual will provide our customers with optimum operational reliability. The data contained herein purports solely to describe the product, and does not create any warranties.

Within the scope of the attached manual, it is impossible to take into account every eventuality that may arise with technical equipment in service. Please consult an ASTS USA local sales representative in the event of any irregularities with our product.

ASTS USA expressly disclaims liability resulting from any improper handling or use of our equipment, even if these instructions contain no specific indication in this respect. We strongly recommend that only approved ASTS USA spare parts are used as replacements.

Copyright© 2009, Ansaldo STS USA, Inc.
1000 Technology Drive, Pittsburgh, PA USA 15219-3120
645 Russell Street, Batesburg, SC 29006
www.ansaldo-sts.com

All rights reserved.

# Revision History

| REV. | DATE | NATURE OF REVISION |
|---|---|---|
| 1 | July, 2009 | Initial Release |
| | | |
| | | |

# Table of Contents

**1. GENERAL INFORMATION ..... 1-1**
1.1. Safety and Regulatory Information ..... 1-1
1.2. FCC Part 15 Compliance ..... 1-1
**2. INTRODUCTION ..... 2-1**
2.1. TransPortal Interlock Monitor ..... 2-1
2.2. Feature Overview ..... 2-2
2.2.1. Top Panel Features ..... 2-2
2.2.2. Front Panel Features ..... 2-2
2.3. Electrical and Mechanical Specifications ..... 2-3
2.4. Operating Overview ..... 2-3
2.5. Front Panel Inputs, Outputs, and Controls ..... 2-4
2.5.1. ETH0 and ETH1 ..... 2-4
2.5.2. USB Port ..... 2-4
2.5.3. Serial Ports 1 and 2 ..... 2-4
2.5.4. Power Input ..... 2-5
2.6. Top Panel Keypad/Displays ..... 2-5
2.6.1. Top Panel Keypad ..... 2-5
2.6.2. Top Panel Indicators ..... 2-5
2.6.2.1. Operational State ..... 2-5
2.6.2.2. Alarm Conditions ..... 2-5
2.6.2.3. Communication Status ..... 2-5
2.6.2.4. System Status ..... 2-6
**3. INSTALLATION AND SETUP ..... 3-1**
3.1. Needed for Installation ..... 3-1
3.2. Unpacking and Inspecting the Unit ..... 3-1
3.3. Physical Mounting ..... 3-2
3.4. Connecting Field Wiring ..... 3-2
3.5. Verifying Installation ..... 3-4
3.5.1. Initialization ..... 3-4
3.5.2. Operation ..... 3-4
**4. CONFIGURING THE TRANSPORTAL INTERLOCK MONITOR ..... 4-1**
4.1. Configuring the MICROLOK II for Use with the TransPortal Interlock Monitor ..... 4-1
4.2. Configuring the TransPortal Interlock Monitor Operating Parameters ..... 4-2
4.2.1. Locally Accessing the Embedded Web Server ..... 4-2
4.2.2. Navigating the Embedded Web Server ..... 4-3
4.2.2.1. Ethernet Tab ..... 4-4
4.2.2.2. Networking Tab ..... 4-6
4.2.2.3. Terminal Servers Tab ..... 4-9
4.2.2.4. Status Tab ..... 4-12
4.2.2.5. Update Tab ..... 4-13
4.2.2.6. Security Tab ..... 4-13

4.3. Configuring SNMP Event Traps ..... 4-13
4.3.1. Generating the MICROLOK II Events File ..... 4-13
4.3.2. Transferring the mlevents.txt File to the TransPortal Interface Monitor ..... 4-15
4.3.2.1. Using a Windows-Based Computer ..... 4-15
4.3.2.2. Using a Linux Computer ..... 4-17
4.3.3. SNMP Trap Timestamp File ..... 4-18
4.4. Invoking the MICROLOK II Development System ..... 4-18
4.4.1. Locally at the TransPortal Interlock Monitor ..... 4-18
4.4.1.1. Configuring the Local Computer ..... 4-19
4.4.1.2. Running the MICROLOK II Development System ..... 4-21
4.4.2. Remotely from a Computer Network Workstation ..... 4-24
**5. SUPPORT AND MAINTENANCE ..... 5-1**
**6. GLOSSARY, ABBREVIATIONS, AND ACRONYMS ..... 6-1**

# List of Figures

Figure 2-1. TransPortal Interlock Monitor ..... 2-1
Figure 3-1. Typical Input/Output Connections ..... 3-2
Figure 3-2. Typical Field Wiring ..... 3-3
Figure 4-1. Typical MICROLOK II Settings and Configuration Servlet ..... 4-1
Figure 4-2. Typical Ethernet Tab ..... 4-4
Figure 4-3. Typical Networking Configuration Tab (1 of 2) ..... 4-6
Figure 4-4. Typical Networking Configuration Tab (2 of 2) ..... 4-7
Figure 4-5. Typical Terminal Servers Tab ..... 4-9
Figure 4-6. Typical Status Tab ..... 4-12
Figure 4-7. Typical Update Tab ..... 4-13
Figure 4-8. Typical Security Tab ..... 4-13
Figure 4-9. Typical mlevents.xls File ..... 4-14
Figure 4-10. Typical mlevents.txt File ..... 4-15
Figure 4-11. Typical mlevents.txt File Transfer Login (Windows Computer) ..... 4-16
Figure 4-12. Typical WinSCP Split Screen (Windows Computer) ..... 4-16
Figure 4-13. Typical mlevents.txt File Transfer (Windows Computer) ..... 4-17
Figure 4-14. Typical snmp.trap.timestamp File Location ..... 4-18
Figure 4-15. Typical Local Area Connection Properties ..... 4-19
Figure 4-16. Typical Local Area Connection Properties (General) ..... 4-20
Figure 4-17. Typical Local Area Connection Properties (Authentication) ..... 4-20
Figure 4-18. Typical Serial-to-TCP/IP Converter Configuration ..... 4-21
Figure 4-19. Typical Serial-to-TCP/IP Converter I/O Options Configuration ..... 4-21
Figure 4-20. Typical Serial-to-TCP/IP Converter (Activated) ..... 4-22
Figure 4-21. Typical MICROLOK II Development System Communications Pop-up ..... 4-22
Figure 4-22. Typical MICROLOK II Development System Communications Setup ..... 4-23
Figure 4-23. Typical MICROLOK II Development System Site Display ..... 4-23
Figure 4-24. Typical MICROLOK II Development System Main Menu ..... 4-24
Figure 4-25. Typical Network Dashboard Screen ..... 4-25

# List of Tables

Table 2-1. Operating Specifications ..... 2-3
Table 2-2. Mechanical Specifications ..... 2-3
Table 3-1. Active Top Panel LED Indicators ..... 3-4

# 1. GENERAL INFORMATION

## 1.1. Safety and Regulatory Information

Read and thoroughly understand this manual before attempting any of the procedures listed. Pay particular attention to:

**CAUTION**

and

**WARNING**

These headings may appear throughout this manual. Caution statements indicate conditions that could cause damage to equipment. Warning statements indicate conditions that could cause physical harm, serious injury, or loss of life. Always observe standard precautions familiar to trained electrical technicians. Always adhere to all safety regulations stipulated by the railroad.

## 1.2. FCC Part 15 Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not, installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at user's own expense.

Operation is subject to the following two conditions: (1) this device may not cause harmful interference and (2) this device must accept any interference received including interference that may cause undesired operation. This Class A digital apparatus meets all requirements of the Canadian interference causing equipment regulations.

This Category II radiocommunication device complies with Industry Canada Standard RSS-310. Ce dispositif de radiocommunication de categorie II respecte la norme CNR-310 d'Industrie Canada.

AnsaldoSTS

# 2. INTRODUCTION

The Ansaldo STS USA, Inc. (ASTS USA) TransPortal™[1] Interlock Monitor (TIM) is a comprehensive status monitoring and reporting device capable of remotely monitoring the ASTS USA MICROLOK®[2] II controller (MLK). The TIM is typically installed at field locations where timely on-site access to the MLK is a concern.

This document contains information for the installation, setup, and use of a TIM.

ASTS USA is committed to providing support and assistance to assure that the quality and the functionality of both the equipment and the network exceeds your expectations. In fulfilling that objective, we encourage you to contact us regarding any difficulties or additional needs you may encounter. The ASTS USA technical support organization is available 24 hours per day at (800) 652-7276 (See Section 5).

## 2.1. TransPortal Interlock Monitor

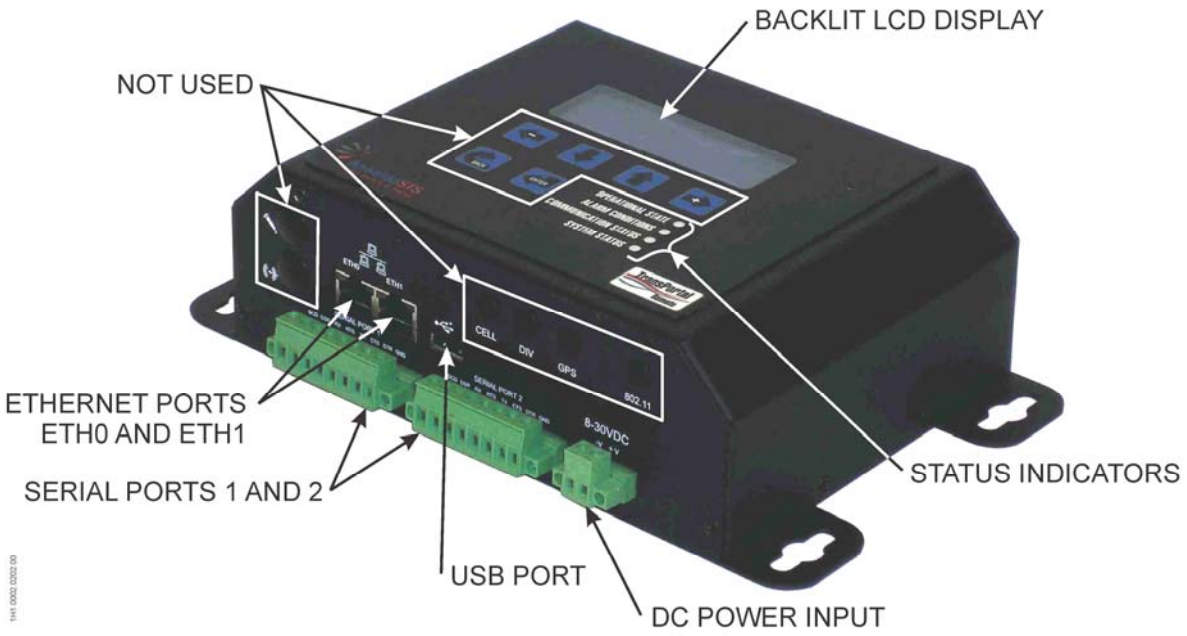



**Figure 2-1. TransPortal Interlock Monitor**

The MLK constantly checks system operational parameters and maintains an internal log file of important event, warning, and error conditions. Maintainers and technicians typically need to use the MICROLOK II Development System application (running on a laptop computer connected at the MLK) to view and react to these logged indications. Where timely access to remote MLK

[1] TransPortal™ is a trademark of Ansaldo STS USA, Inc.
[2] MICROLOK® is a registered trademark of Ansaldo STS USA, Inc.

locations is not practical, the TIM may be used to monitor the MLK remotely and provide notification of these MLK events. This minimizes the need for travel to very remote sites.

The TIM connects to the MLK using a serial interface. The TIM also connects to an SNMP host to deliver the events detected within the MLK. When connected, the TIM continuously polls the MLK for its current log file and examines the file for new, reportable events.

Using a Microsoft Excel spreadsheet tool to establish which events should be detected, and under what conditions, enabled events are uniquely translated to an "SNMP Trap" protocol and sent to the host application over an IP-based Wide Area Network (WAN) connection.

Because the TIM maintains a continuous connection to the host application, a facility is provided that allows distant maintainers and technicians to remotely invoke many of the MICROLOK II Development System functions over the network, further minimizing the need to visit remote sites when researching or remedying a MLK related system anomaly.

## 2.2. Feature Overview

The top panel of the TIM contains a backlit LCD display unit, six local menu navigation buttons, and four LED status indicators. The front panel of the TIM contains two Ethernet ports, one USB port, two serial ports, and one DC power input connector. See Figure 2-1.

### 2.2.1. Top Panel Features

The top panel LCD display shows current IP address information for the TIM WAN and SNMP host connections. The local menu navigation buttons are not used in this TIM application. All active TIM features are accessed remotely using a WAN connection with the SNMP host or locally using a laptop computer connected to the TIM front panel.

Only two of the four bi-color (red/green) LED indicators are used in this TIM application: Communication Status and System Status. The TIM tests all four LEDs during powerup (solid red and solid green), then controls the active LEDs in this TIM application.

### 2.2.2. Front Panel Features

The front panel Ethernet RJ-45 connectors allow connecting the TIM to a WAN and laptop computer. ETH0 is typically used for connecting a laptop computer for configuring the unit. ETH1 is typically used for connecting the unit to a WAN for data communication. Serial Port 2 is used for data communication with the MLK; Serial Port 1 is not used in this TIM application. The 8–30VDC connector receives TIM operating power from the site power distribution system. The remaining connectors on the front panel are not used in this application.

## 2.3. Electrical and Mechanical Specifications

The TIM meets all applicable environmental, EMI, and vibration tolerance specifications for Class C equipment. Table 2-1 and Table 2-2 list the TIM specifications.

**Table 2-1. Operating Specifications**

| PARAMETER | VALUE |
|---|---|
| System Power Source Voltages | 8 to 30VDC, 10W |
| Temperature Range | –40 to +70°C |
| Humidity | 0% to 95% non-condensing per AREMA 11.15.1 |
| Vibration | Per AREMA 11.15.1 |
| EMI | Per AREMA 11.15.1 |
| Isolation and Protection | Per AREMA 11.3.3 |

**Table 2-2. Mechanical Specifications**

| PARAMETER | VALUE |
|---|---|
| Height | 2.625 inches |
| Width | 9.5 inches including mounting flanges |
| Depth, including connectors | 7.5 inches |
| Recommended clearance depth (including cables) | 9.0 inches |
| Weight | 3 lbs. |
| Mounting | Wall or Shelf Flange Mount, Horizontal |

## 2.4. Operating Overview

The MLK continuously monitors various operational parameters and maintains an internal log of important system event, warning, and error conditions. The TIM looks for the occurrence of pre-configured SNMP Trap/Inform events within this log. If a configured Trap/Inform event is detected, the TIM captures data from the controller log and triggers a message to a host system database. Notifications of the Trap/Inform event may be delivered by the host to pre-configured recipients by e-mail, fax, text message, or accessed through direct access to the host system.

The TIM contains an embedded web server. This server allows users to access alarm and status data, remotely reset the MLK, and perform basic setup of the TIM on the network using a web browser interface. Optionally, the device may be connected to any wired IP network for communication with a host system.

Capable of communicating over any type of public or private, wireless or wireless IP-based WAN, the TIM transmits SNMP-based Trap/Inform messages when any alarm situation is confirmed, and delivers periodic operating information and health check messages. SNMP-based TIM devices are configured to deliver SNMP Trap/Inform encoded alarm and status messages to properly configured SNMP host applications.

The TIM contains a powerful CPU and communication platform (called ZyWAN), event-driven architecture, and a flexible, publish-subscribe network messaging methodology based on IBM WebSphere™, maximizing the system's ability to interoperate with other databases and existing office systems. This application of the TIM currently uses SNMP, rather than publish-subscribe and WebSphere capabilities.

## 2.5. Front Panel Inputs, Outputs, and Controls

See Figure 2-1.

### 2.5.1. ETH0 and ETH1

The front panel Ethernet ports may be used for a variety of purposes, including:

- Connecting a laptop or other browser equipped device for locally configuring and controlling the unit.
- As a LAN for connecting other Ethernet based accessories including network cameras, network switches and hubs.
- To connect to a private wired or wireless WAN. Note that this typically requires coordination with the user's IT department to establish necessary secure communications between the private network and the shared TIM host. Contact ASTS USA Customer Support for assistance for connecting the TIM to a private wired or wireless network.
- Numerous security, firewall, routing, and server functions can be established for the front panel Ethernet ports. Contact ASTS USA customer support for additional assistance.

### 2.5.2. USB Port

The front panel USB port is primarily used for downloading and capturing information, and for introducing new feature and software updates into the TIM.

### 2.5.3. Serial Ports 1 and 2

Serial Ports 1 and 2 have a number of uses. They are typically used to provide terminal server pass-through services to external, serially connected equipment. This allows secure remote access to these legacy devices, reducing the trips that must otherwise be taken to remote sites. In this application of the TIM, a serial port also provides the data connection to the MLK.

### 2.5.4. Power Input

The TIM is powered by 8–30VDC. Although the power input is fully isolated and protected against reverse battery connection, observe the polarity when connecting power to avoid damage to the unit.

## 2.6. Top Panel Keypad/Displays

Due to the persisted IP network connection that the unit maintains, all monitored status, alarm information, and configuration settings can be managed over the network (Remote Operation). When on-site with the unit (Local Operation), the best way to interact with the unit is to plug a browser-equipped computer into the unit and interact with its embedded server.

### 2.6.1. Top Panel Keypad

The keypad located on the top panel is not used in this application.

### 2.6.2. Top Panel Indicators

Four red-green LED indicators are on the TIM top panel. At a glance, these indicators display the status of four major functional areas of the unit. Typically, if any of these indicators is red rather than green, there is some condition or situation that needs to be explored, typically using the Keyboard/Display navigation or a browser-equipped computer and interacting with the embedded server inside the unit.

#### 2.6.2.1. Operational State

The Operational State LED indicator is not used in this TIM application.

#### 2.6.2.2. Alarm Conditions

The Alarm Conditions LED indicator is not used in this TIM application.

#### 2.6.2.3. Communication Status

The Communication Status LED shows the status of the TIM-to-MLK (not WAN) connection. Communication status verifies (green) that the TIM has established a valid serial link to the MLK. Periodically the TIM may be momentarily disconnected when processing large event logs from the MKL. During these brief periods and during TIM startup (which can last for 90-120 seconds), the TIM continues attempting reconnection with the MLK, and the Communication Status LED will be red. The status of the serial connection between the TIM and the MLK is also communicated to the host system using specific SNMP traps.

#### 2.6.2.4. System Status

The System Status LED summarizes the health of the unit's internal operation. It is typically green, indicating that all systems are functioning nominally. If the System Status indicator turns red, it is a sign that one or more of the following conditions has been detected:

- A corrupted or erroneous property file or internal error log entry.
- An application bundle is not properly running or has not started.
- The event recorder memory is missing or not functioning properly.

While this does not necessarily mean that the unit is not functioning, it does suggest that the underlying conditions should be examined. To do so, please contact ASTS USA Customer Support for assistance.

# 3. INSTALLATION AND SETUP

This section provides detailed instructions for the proper installation and setup of the TransPortal Interface Monitor (TIM). Included are steps to perform the following:

1. Gather the tools and devices needed for installation.
2. Unpack and inspect the TIM.
3. Mount the TIM.
4. Connect the field wiring.
5. Connect the power source and power up the unit for the first time.

You are encouraged to read this section in its entirety before attempting installation of the TIM.

## 3.1. Needed for Installation

There are several important tools and devices necessary to properly install the TIM:

1. Drill and appropriate drill bits for creating a 3/8-inch hole for mounting the TIM.
2. A small screwdriver with a 1/8-inch (or smaller) blade for securing wiring in the TIM terminal strips.
3. A digital volt meter to verify power connections and monitored input connections.
4. A Windows-based computer to configure the unit using the embedded web server. The computer should use either an Internet Explorer (version 6 or later) or Mozilla Firefox (version 2 or later) browser. Other browsers may be used, but may not work as described in this document.

   While the basic operating information and status of inputs can be accessed over the WAN, it is strongly recommended that a browser-equipped computer be used to configure the unit in the easiest and most comprehensive manner.

## 3.2. Unpacking and Inspecting the Unit

The basic TIM package typically contains the following items in addition to the unit:

1. CAT5 Crossover Network Cable (for connecting a browser-equipped Windows computer to the unit's embedded server configuration applications)
2. TIM Service Manual (this document)

Great care is taken in packaging each item to prevent damage in shipment; however, damage can sometimes occur and it is not advisable to install or attempt to operate damaged equipment or equipment with suspected damage. Carefully inspect each package at time of receipt for signs of physical damage. Report any suspected damage claims to the shipper and to Customer Support.

## 3.3. Physical Mounting

The TIM may be mounted horizontally on a shelf or vertically on a wall. Select a panel, wall, plywood back plane, or shelf in a location where it will not be exposed to harsh weather extremes or moisture. If possible, the unit should be mounted at a height to allow easy access to the display, controls, and I/O connections. It is recommended that the unit be installed at least 18-inches away from high-voltage power sources or other equipment.

The TransPortal should be mounted inside a separate, weatherproof enclosure (rated NEMA 4, 4X or better) if it is to be installed outdoors.

## 3.4. Connecting Field Wiring

See Figure 3-1 for typical input/output connections and Figure 3-2 for typical field wiring.

1. Connect the WAN cable to the ETH1 (typical) RJ-45 jack.
2. Connect the Ethernet crossover cable (supplied with the unit) from the DB-9 (DTE) connector on the MICROLOK II CPU cardfile PCB to Serial Port 2 (typical) on the TIM.

**NOTE**

> Some applications may assign the MLK DTE port to top connector wiring on the CPU cardfile PCB. If so, connect these wires to Serial Port 2 (typical) on the TIM; no crossover cable is required.

3. Connect the DC input power to the 8–30VDC terminal strip.

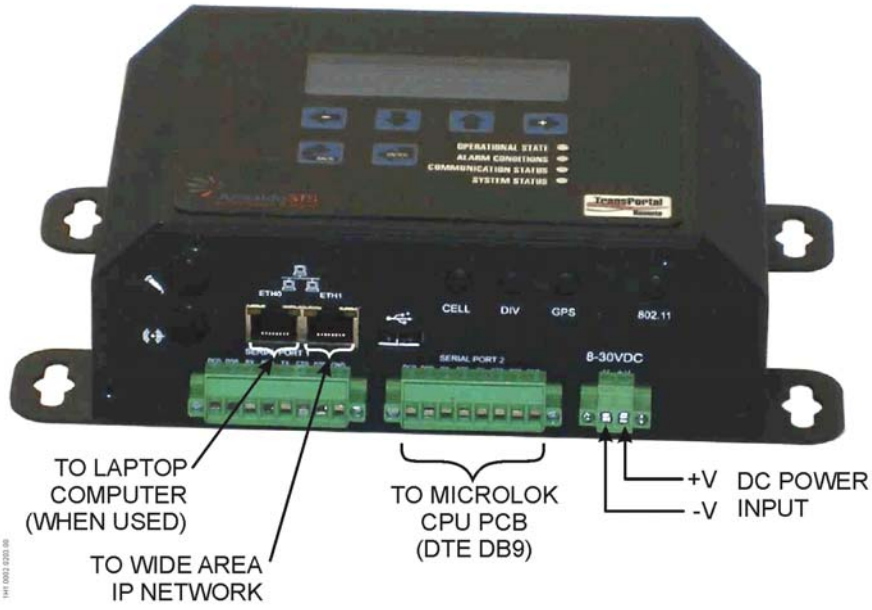



**Figure 3-1. Typical Input/Output Connections**

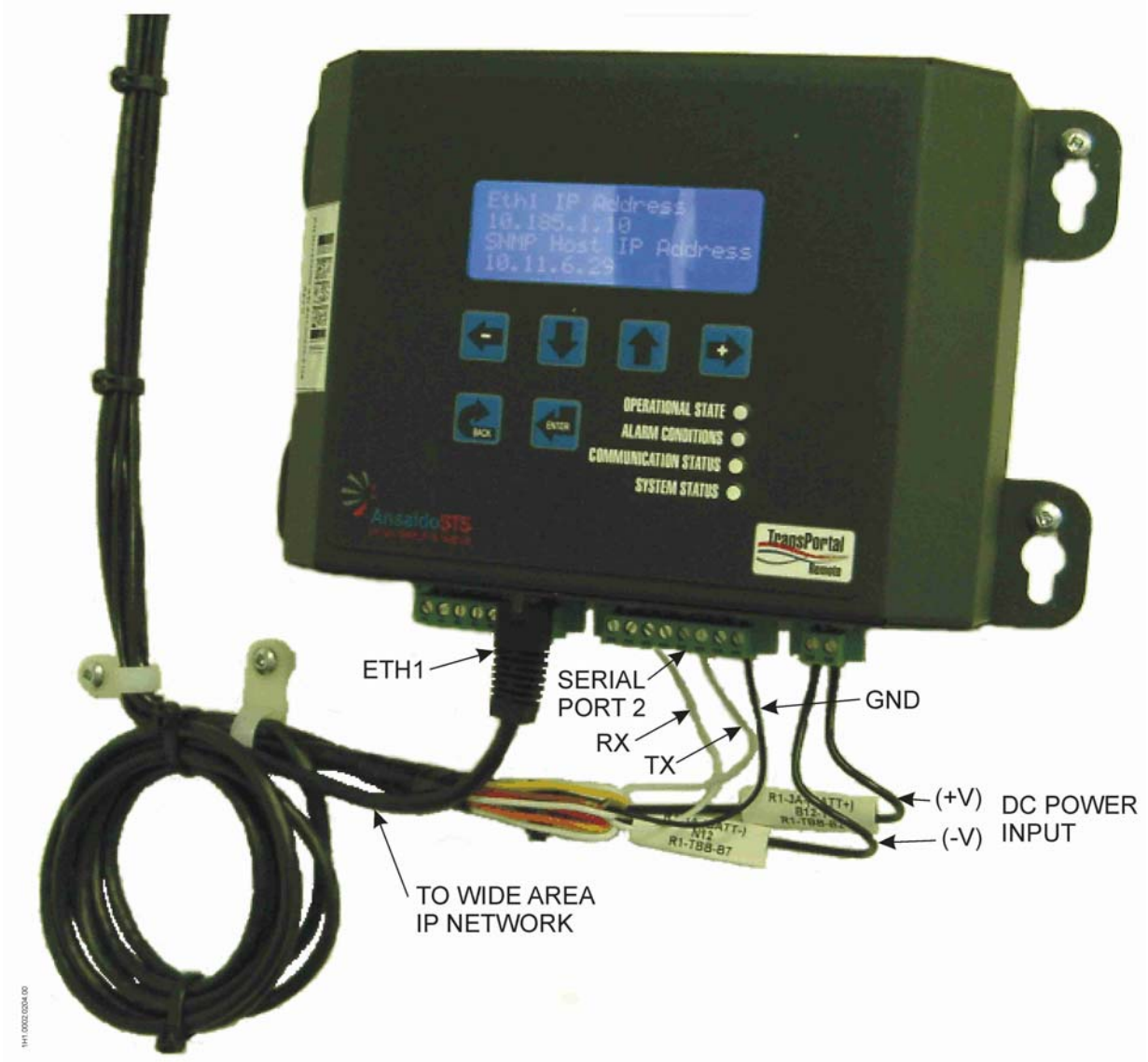



**Figure 3-2. Typical Field Wiring**

## 3.5. Verifying Installation

The TransPortal provides visual confirmation of connectivity and operation using a top panel backlit LCD display and bi-color LED status indicators. See Figure 2-1.

### 3.5.1. Initialization

As the TransPortal powers up, the LCD top panel display typically shows the following;

*TransPortal Remote*
*Monitoring Network*
*Ansalso-STS USA*
*Initializing…*

As part of the power up sequence, the TIM checks operation of the four bi-color LED status indicators on the top panel of the unit. Each LED state is tested (OFF, Red, and Green).

### 3.5.2. Operation

Following initialization, the LCD display shows the IP addresses of the Ethernet connection between the TIM (typically ETH1) and the host server. A typical display is shown below.

*Eth1 IP Address*
*192.168.1.110*
*SNMP Host Address*
*192.168.1.111*

During operation, only the Communication Status and System Status LED indicators are used in this application. Table 3-1 describes the TIM status for each state of the active LED indicators in this application.

**Table 3-1. Active Top Panel LED Indicators**

| ACTIVE LED | DESCRIPTION |
|---|---|
| Communication Status LED | |
| Green | Connected to and communicating with the MICROLOCK II controller |
| Red | MICROLOK II controller communication link pre-empted or lost |
| Off | Communication software not running |
| System Status LED | |
| Green | System software running |
| Red | System software not running |

# 4. CONFIGURING THE TRANSPORTAL INTERLOCK MONITOR

This section provides detailed instructions for configuring the TransPortal Interlock Monitor (TIM) for operation. By this time, the unit is presumed to be physically installed, that a working network connection has been established, and that the unit has been turned on, initialized and is active. The Communication and System Status LEDs should show "all green" status on the top panel of the unit.

This section provides guidance on how to perform the following configuration steps:

1. Configuring the MICROLOK II controller (MLK) for use with the TIM using the embedded servlet.
2. Configuring TIM operating parameters using the embedded web server.
3. Configuring SNMP Event Traps using the Microsoft Excel spreadsheet tool.

## 4.1. Configuring the MICROLOK II for Use with the TransPortal Interlock Monitor

The MLK configuration can be changed using the TIM internal configuration servlet. The servlet can be accessed locally through the Ethernet jack (typically ETH0) on the TIM or remotely through the WAN port (typically ETH1), by adding the port and directory information (typically ":10000/microlok") to the IP address of the TIM. See Figure 4-1.

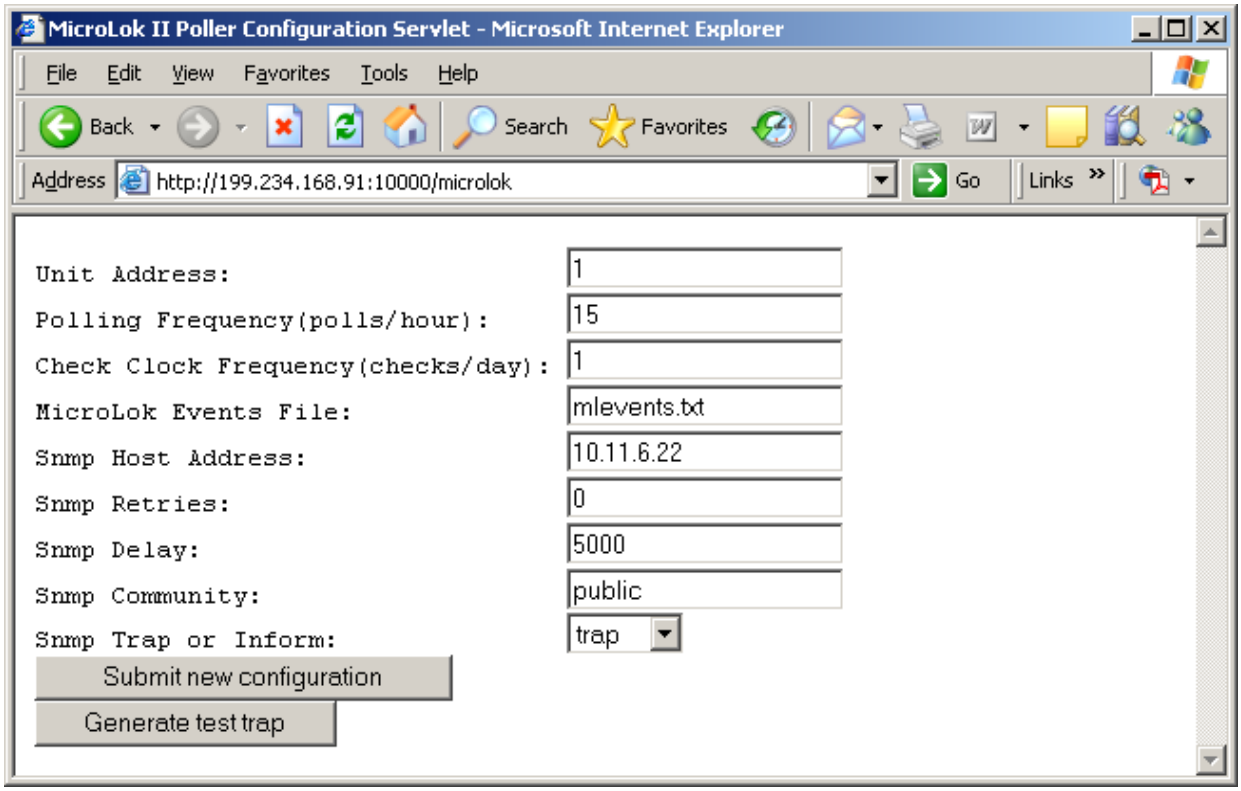



**Figure 4-1. Typical MICROLOK II Settings and Configuration Servlet**

When accessed by either method, the browser presents the following fields and buttons contained in the servlet:

- **Unit Address** – Address of the unit connected to the MLK; typically set to 1 or 2.
- **Polling Frequency** – Number of times the Unit will poll the MLK event log (per hour) for new event information; typically set to 1 or 2 times per hour.
- **Check Clock Frequency** – Number of times the Unit will check the MLK system clock (per day) for accuracy.
- **MICROLOK Events File** – File containing information of specific MLK events that are to be identified and the parameters for determining whether qualifying event information should be converted to SNMP Trap/Inform format and forwarded over the WAN to the SNMP Host application (or manager).
- **SNMP Host Address** – The IP address of the SNMP manager that will receive any generated SNMP traps/informs.
- **SNMP Retries** – The number of SNMP trap/inform retries.
- **SNMP Delay** – The SNMP trap/inform delay in milliseconds.
- **SNMP Community** – The SNMP community associated with any generated SNMP traps/informs.
- **SNMP Trap or Inform** – Send SNMP traps or SNMP informs.
- **Submit new configuration** – Button to submit any changes made to the configuration fields.
- **Generate test trap** – Button to generate and send a test trap to the SNMP manager.

## 4.2. Configuring the TransPortal Interlock Monitor Operating Parameters

The embedded web server interface provides a full view of all conditions monitored by the MLK, and control over all configurable data fields that define the behavior of the TIM. Typically, the web server should be accessed by plugging a laptop computer directly into the TIM. In a typical setup, Ethernet port ETH0 is left empty and is used to establish this user interface. Configuration may also be accomplished remotely when the TIM is connected to a wired WAN (typically Ethernet port ETH1).

### 4.2.1. Locally Accessing the Embedded Web Server

To access the embedded web server:

1. Connect a laptop computer to the TIM, typically using Ethernet port ETH0.
2. Open a web browser window (Internet Explorer or Mozilla Firefox recommended; See Section 3.1.) on the laptop.
3. Navigate the browser to the IP address of the unit, typically by entering 192.168.1.1 in the browser address field followed by the Enter key.

### 4.2.2. Navigating the Embedded Web Server

The embedded web server has a number of navigational tabs along the top of the home page. Each tab takes you to a different web page, providing convenient local access to configure the behavior of the TIM. On initial access, the Status configuration tab (See Section 4.2.2.4.) is shown by default.

- **Cellular** Not used in this TIM application
- **Ethernet** Configure Ethernet ports ETH0 and ETH1 (See Section 4.2.2.1)
- **Wifi** Not used in this TIM application
- **Networking** Open and configure communication ports (See Section 4.2.2.2)
- **GPS** Not used in this TIM application
- **Terminal Clients** Not used in this application
- **Terminal Servers** Enable and configure terminal servers (See Section 4.2.2.3)
- **Status** View software revision and hardware configuration data (See Section 4.2.2.4)
- **Update** Update the TIM URL (See Section 4.2.2.5)
- **Security** Change web password for TIM access (See Section 4.2.2.6)

A description of each active web page used in this TIM application and how to view or configure the page follows.

#### 4.2.2.1. Ethernet Tab

The Ethernet tab allows configuring Ethernet ports ETH0 and ETH1. See Figure 4-2 for typical screens and configuration data. Typically, ETH1 is used for connecting the TIM with the WAN and ETH0 is used for local access to the TIM using a laptop computer. To save configuration changes, select "Submit New Configuration" before leaving the page.

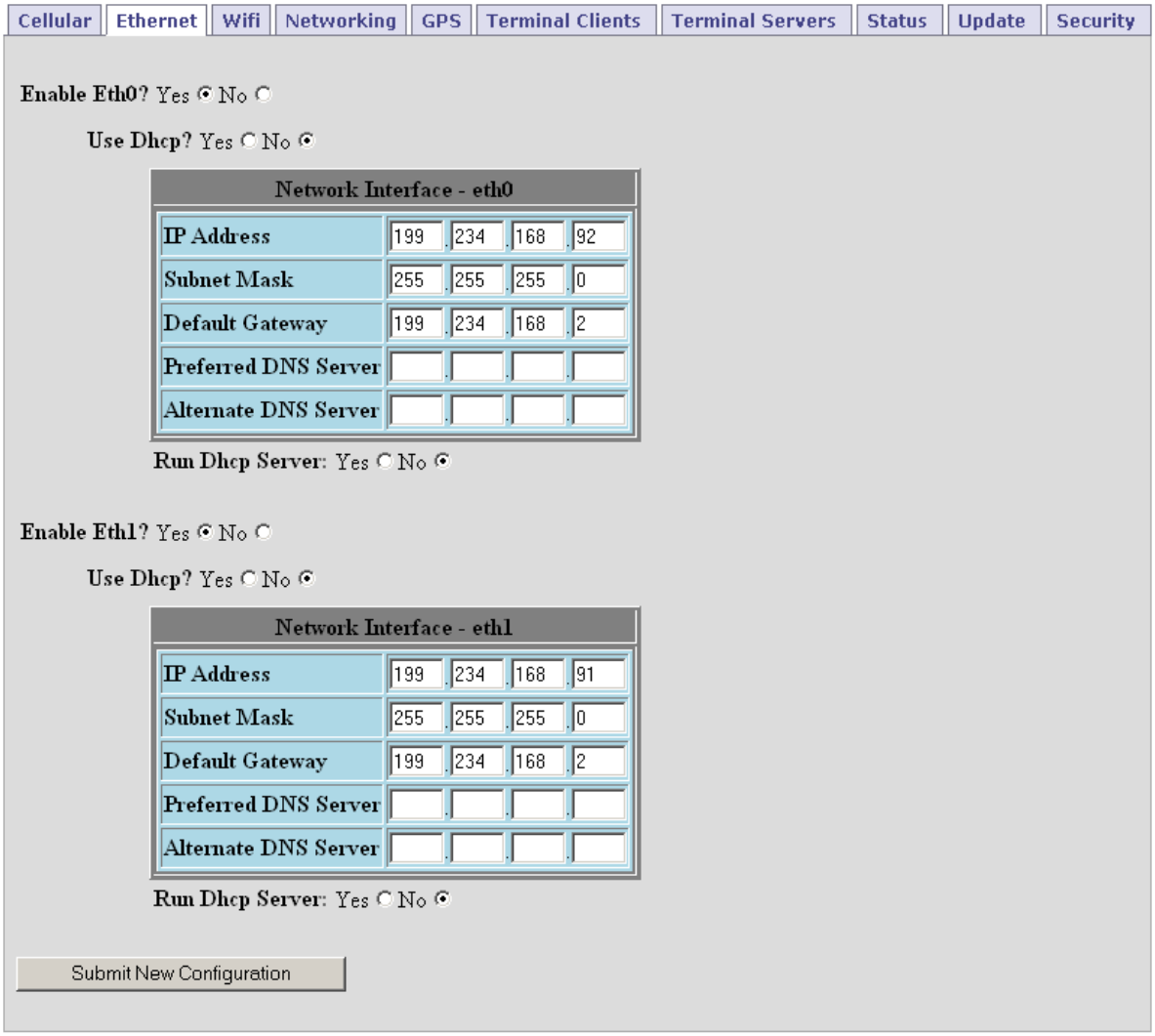



**Figure 4-2. Typical Ethernet Tab**

**NOTE**

The data shown in these web page views are only ***representative*** of the configuration data required for a specific interlocking. Each TIM must be configured with ***interlocking-specific data*** for that location.

Each TIM must also be configured with ***specific*** network- and SNMP-host interface parameters for that location.

- **Enable ETH0? (ETH1?)** Select "Yes" and configure each port as described below:

  **Use DHCP?** – Select 'No" for this TIM application and enter the following:

  ***IP Address*** – Enter the numeric address for the TIM. Each field must be a whole number between 1 and 255.

  ***Subnet Mask*** – Enter the subnet mask for this network. Each field must be a whole number between 1 and 255.

  ***Default Gateway*** – Enter the numeric address of the default gateway (if used) for this network. Each field must be a whole number between 1 and 255.

  ***Preferred DNS Server*** – Enter the numeric address of the preferred DNS server (if used) for this network. Each field should be a whole number between 1 and 255. If no preferred DNS server is used, each field should be zero (0) or blank.

  ***Alternate DNS Server*** – Enter the numeric address of the alternate DNS server (if used) for this network. Each field should be a whole number between 1 and 255. If no alternate DNS server is used, each field should be zero (0) or blank.

- **Run DHCP Server:** – Select "No" for this TIM application.

### 4.2.2.2. Networking Tab

The Networking tab allows opening up to five inbound ports, and enabling NAT and time synchronization. See Figure 4-3 and Figure 4-4 for typical screens and configuration data. To save configuration changes, select Submit New Configuration" before leaving the page.

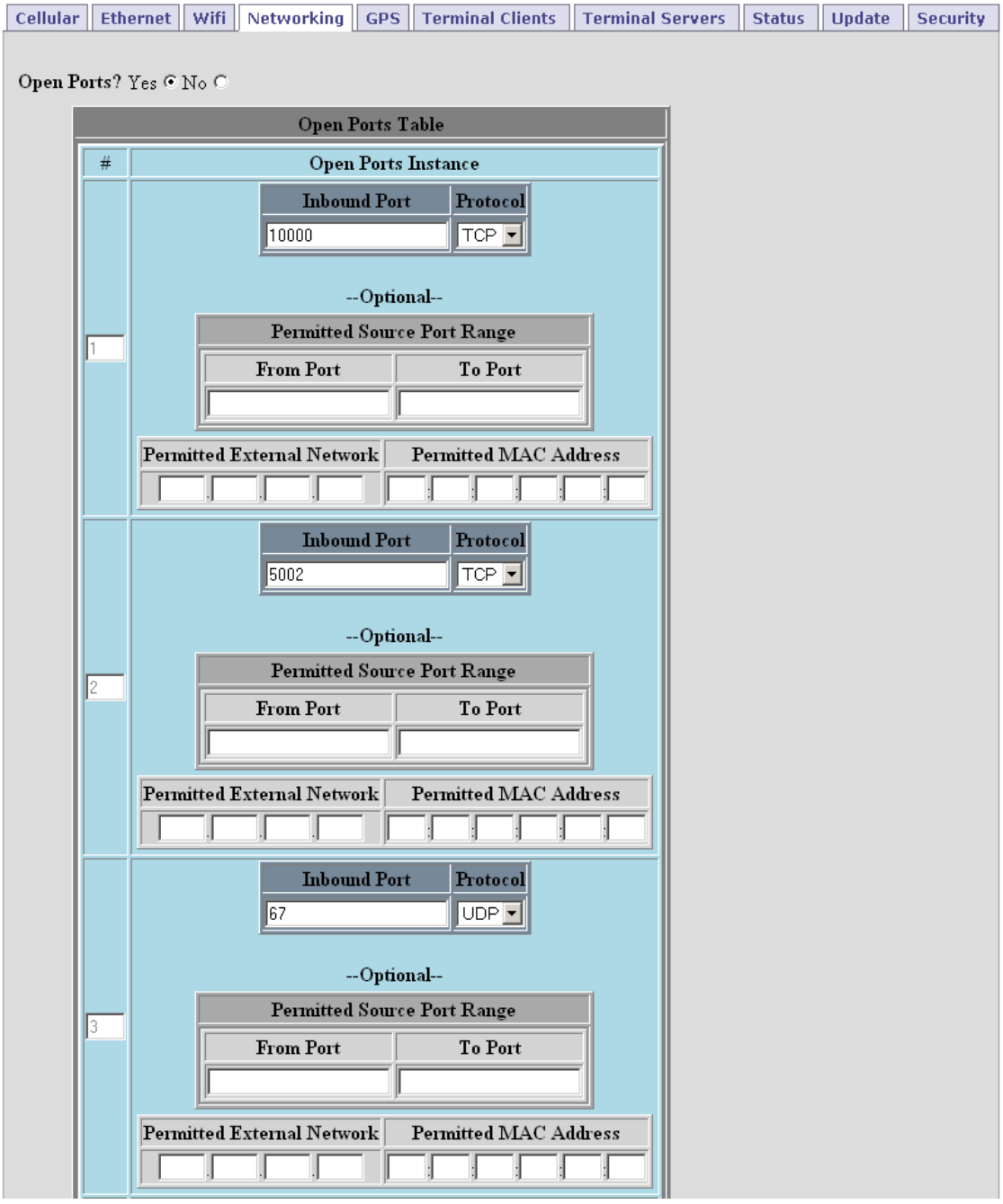



**Figure 4-3. Typical Networking Configuration Tab (1 of 2)**

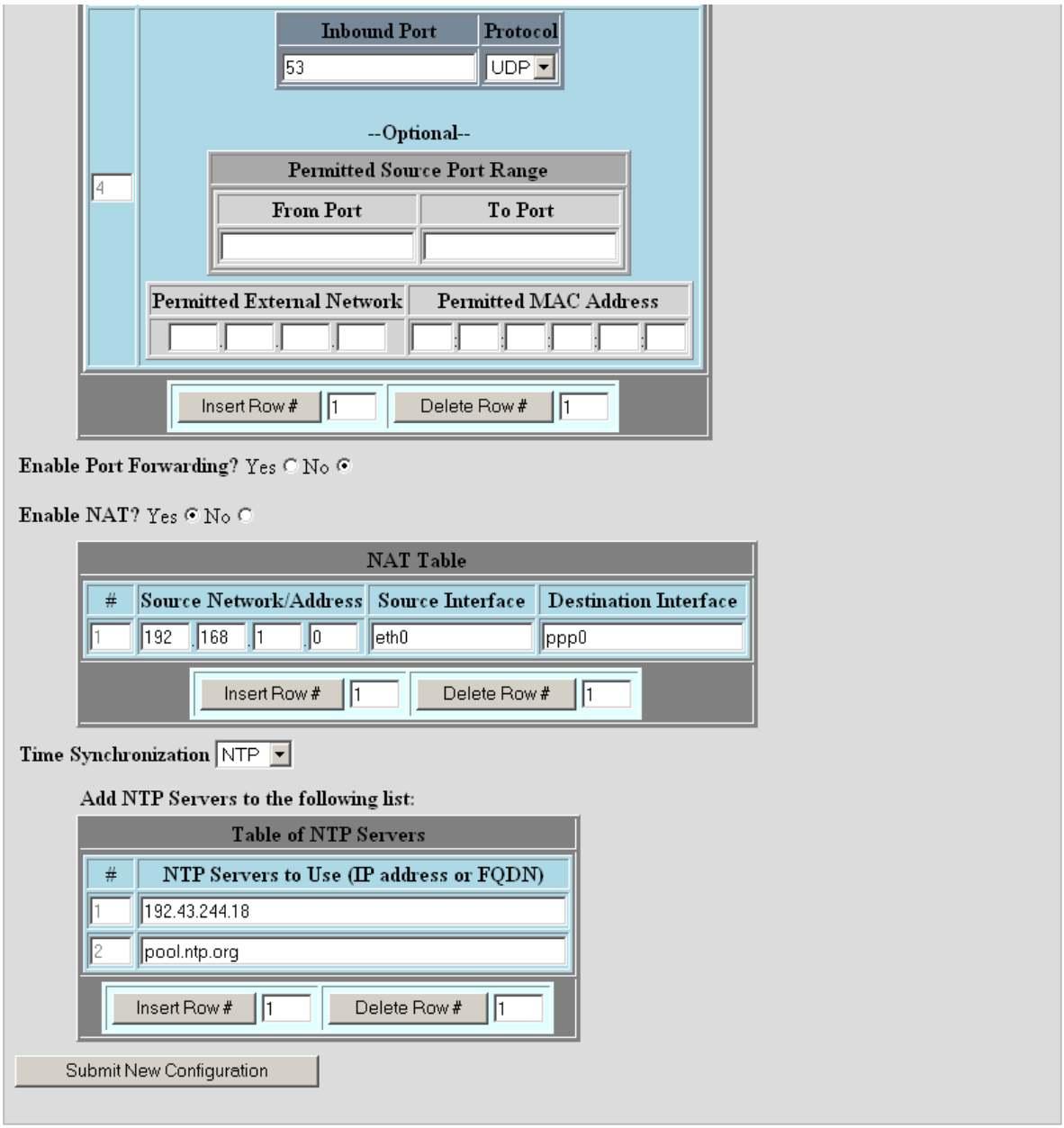



**Figure 4-4. Typical Networking Configuration Tab (2 of 2)**

**NOTE**

The data shown in these web page views are only ***representative*** of the configuration data required for a specific interlocking. Each TIM must be configured with ***interlocking-specific data*** for that location.

Each TIM must also be configured with ***specific*** network- and SNMP-host interface parameters for that location.

- **Open Ports Table** – Allows viewing and configuring available inbound ports. Only three ports (1, 2, and 3) are used in this TIM application.

  ***Inbound Port*** – Enter the numeric address for each active incoming connection. Valid port addresses range from 1 to 65535.

  ***Protocol*** – Select the port protocol from the dropdown list (TCP or UDP).

- **Enable Port Forwarding** – Not used in this TIM application.

- **Enable NAT** – Select "Yes" for this TIM application and enter the following:

  ***Source Network Address*** – Enter the numeric IP address for the source to be translated. Each field should be a whole number between 1 and 255.

  ***Source Interface*** – Enter the name of the network interface (typically "eth0") containing the source network address to be translated.

  ***Destination Interface*** – Enter the name of the network interface (typically "ppp0") that is to receive the translation output.

- **Time Synchronization** – Select the desired synchronization method and time server(s).

  ***Time Synchronization*** – Only the NTP method for synchronizing time is available in this TIM application.

  ***NTP Servers to Use*** – Enter the IP address or FQDN of the server(s) the TIM should synchronize with.

### 4.2.2.3. Terminal Servers Tab

The Terminal Servers tab allows configuring a listening port for inbound TCP/IP connection, allowing network communication directly to a local serial port. See Figure 4-5 for a typical screen and configuration data. To save changes, select "Submit New Configuration" before leaving the page.

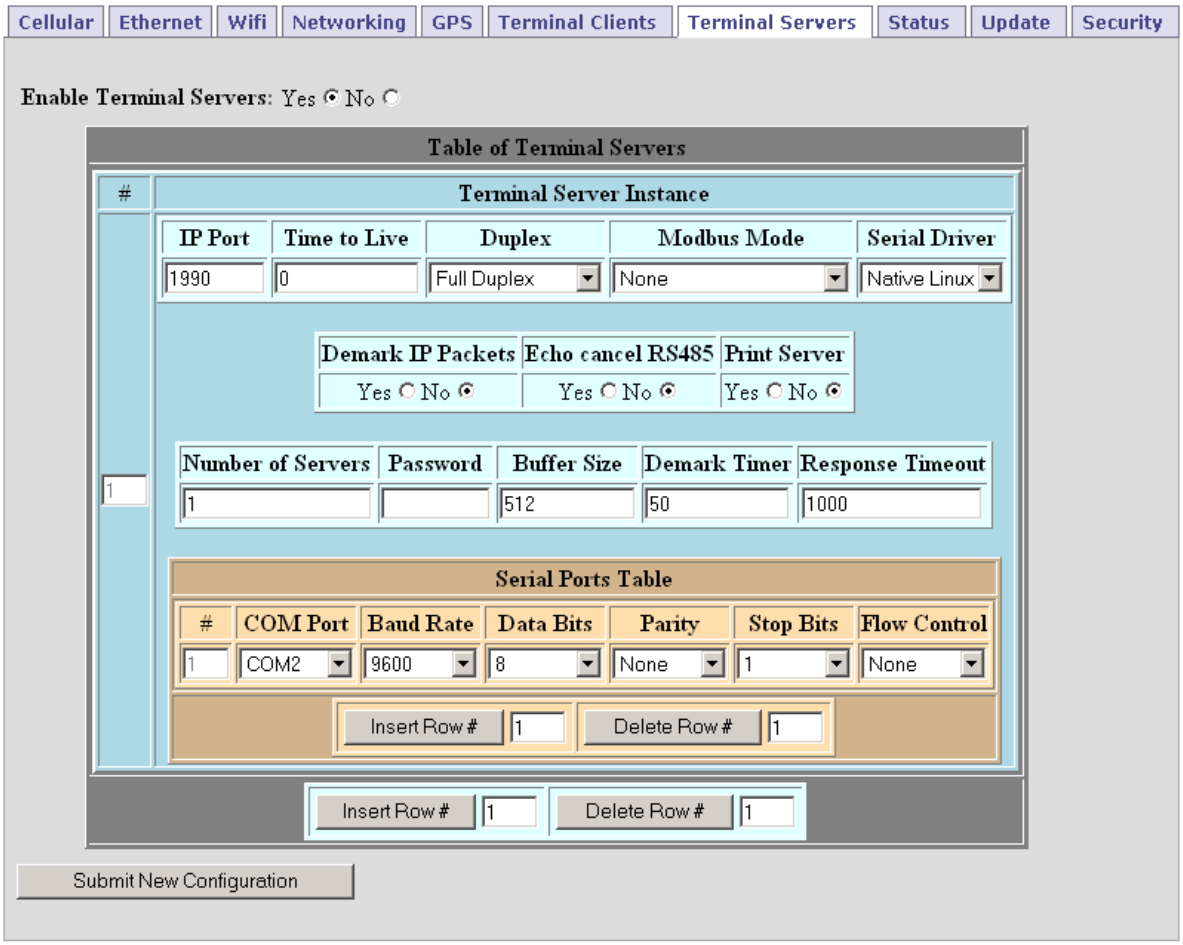



**Figure 4-5. Typical Terminal Servers Tab**

**NOTE**

The data shown in these web page views are only ***representative*** of the configuration data required for a specific interlocking. Each TIM must be configured with ***interlocking-specific data*** for that location.

Each TIM must also be configured with ***specific*** network- and SNMP-host interface parameters for that location.

- **Enable Terminal Servers** – Select "Yes" to enable and view the Table of Terminal Servers. Typically, only one terminal server needs configured.

- **Terminal Server Instance Table**

  ***IP Port*** – Enter the IP port number (1 to 65535) to be used for the incoming TC/IP connection to the TIM from the network client.

  ***Time to Live*** – Enter the maximum time (in seconds) that the TIM should keep this connection open while there is no incoming activity from the network client. If this time is exceeded, the TIM will close the connection to the network client.

  ***Duplex*** – Select "Full Duplex" (typical) for this TIM application.

  ***Modbus Mode*** – Select "None" (typical) for this TIM application

  ***Serial Driver*** – Select "Native Linux" (typical) for this TIM application.

  ***Demark IP Packets*** – Select "No" (typical) for this TIM application.

  ***Echo Cancel RS485*** – Select "No" (typical) for this TIM application.

  ***Print Server*** – Select "No" (typical) for this TIM application.

  ***Number of Servers*** – Enter the number of clients (eight maximum) that can connect to this terminal server simultaneously. If set to "1," the terminal server is preemptive (if a second client connects to this port, the previous client is disconnected). If set to three (or more), additional connections will be blocked when the specified number of connections has been made. Select "1" (typical) for this TIM application.

  ***Password*** – (Optional) Enter a password (15 characters maximum) for the terminal server connection. When set, the connection is dropped if the password (case-sensitive) is not entered within one minute of the password prompt.

  ***Buffer Size*** – Enter the maximum size (between 1 and 4095 bytes) allowed in the response to a network client. The actual number of bytes sent may be less if the

Demark Timer expires before the serial butter is full. Enter 512 (typical) for this TIM application.

***Demark Timer*** – Enter the maximum time (from 10 to 30,000 milliseconds) that the TIM should wait for activity on the serial port to cease before sending a response back to the network client (presuming that at least one byte was received). Enter 50 (typical) for this TIM application.

***Response Timeout*** – (This field is ignored unless the "Half Duplex" option is set; it does not apply to this TIM application.) Enter the desired timeout (from 10 to 30000 milliseconds). If a response is not received from the serial port within the specified time, the port is released and the terminal receiver will not read any more serial data until the next request is received. Enter 1000 (typical) for this TIM application.

**Serial Ports Table** – The Serial Ports Table (brown background) is part of the Terminal Server configuration. At least one row in the Serial Ports Table must be configured for the Terminal Server to work properly.

***COM Port*** – Select the serial port (COM2 or COM3) from the drop-down list. To avoid conflicts, this port must *not* be configured for any other use by the TIM. Select "COM2" (typical) for this TIM application.

***Baud Rate*** – Select the desired baud rate (1200 to 115, 200) for the Terminal Server port. Select "9600" (typical) for this TIM application.

***Data Bits*** – Select the number of data bits (5 to 8) to use for the Terminal Server port. Select "8" (typical) for this TIM application.

***Parity*** – Select the parity for use with the port. Select "None" (typical) for this TIM application.

***Stop Bits*** – Select the number of stop bits for use with this port. Select "1" (typical) for this TIM application.

***Flow Control*** – Select the method for use with this port. Select "None" (typical) for this TIM application.

#### 4.2.2.4. Status Tab

The Status tab shows the current status and configuration of the TIM. The data is shown for viewing only, and cannot be changed on this screen. See Figure 4-6 for a typical screen and configuration data.

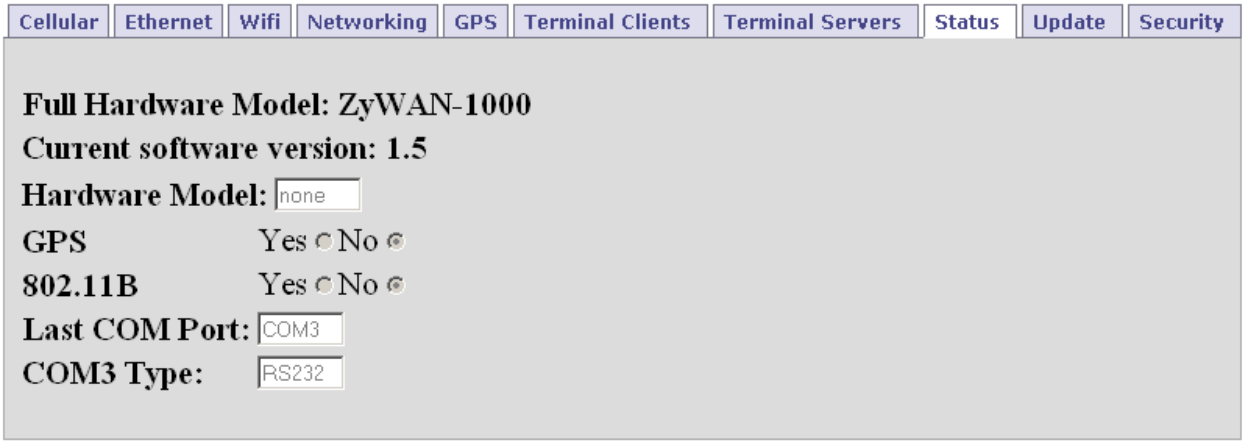



**Figure 4-6. Typical Status Tab**

**Full Hardware Model** – Shows basic hardware data.

**Current Software Version** – Shows current software version.

**Hardware Model** – Shows the type of cellular modem installed. Not applicable for this application.

**GPS** – Shows the type of GPS hardware installed. Not applicable for this application.

**802**.11B – Shows if an 802.11b WiFi module is installed. Not applicable for this TIM application.

**Last COM Port** – Shows the last available COM port in the TIM. This data is used in all other configuration menus where a selection of COM port is allowed.

**COM3 Type** – The COM3 port may be factory-configured as either RS-232 (shown as RS-232) or RS-485/422 (shown as RS-485).

#### 4.2.2.5. Update Tab

The Update tab allows updating the TIM firmware to a later version. See Figure 4-7 for a typical screen. Enter the Uniform Resource Locator (URL) from which an update file may be downloaded. This address must be accessible through one of the configured network interfaces of the TIM. Select "Update ZyWAN" to download and install the update file. The TIM will reboot (if necessary) to complete the installation.

**Figure 4-7. Typical Update Tab**

#### 4.2.2.6. Security Tab

The Security tab allows changing the username and password for accessing the TIM. See Figure 4-8 for a typical screen. Enter the current, and then new, username and password in the fields provided (15 characters maximum for each) in the fields provided. To save changes, select "Change Web Password" before leaving the page.

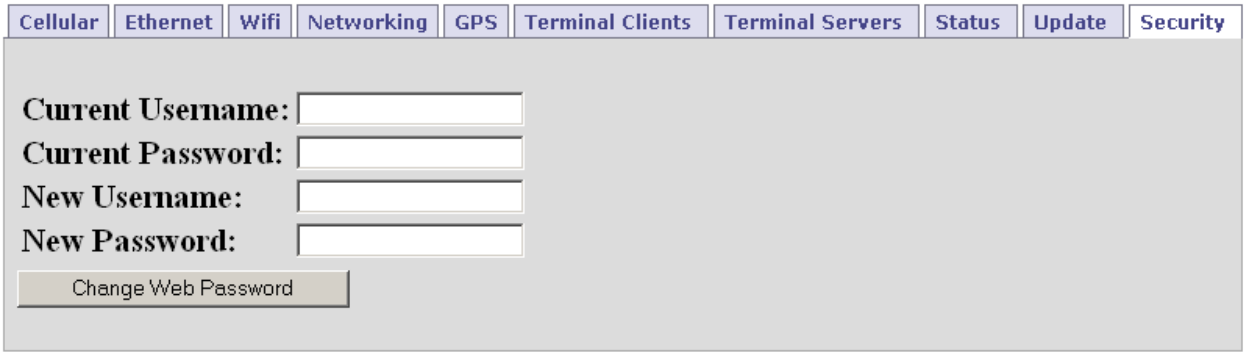



**Figure 4-8. Typical Security Tab**

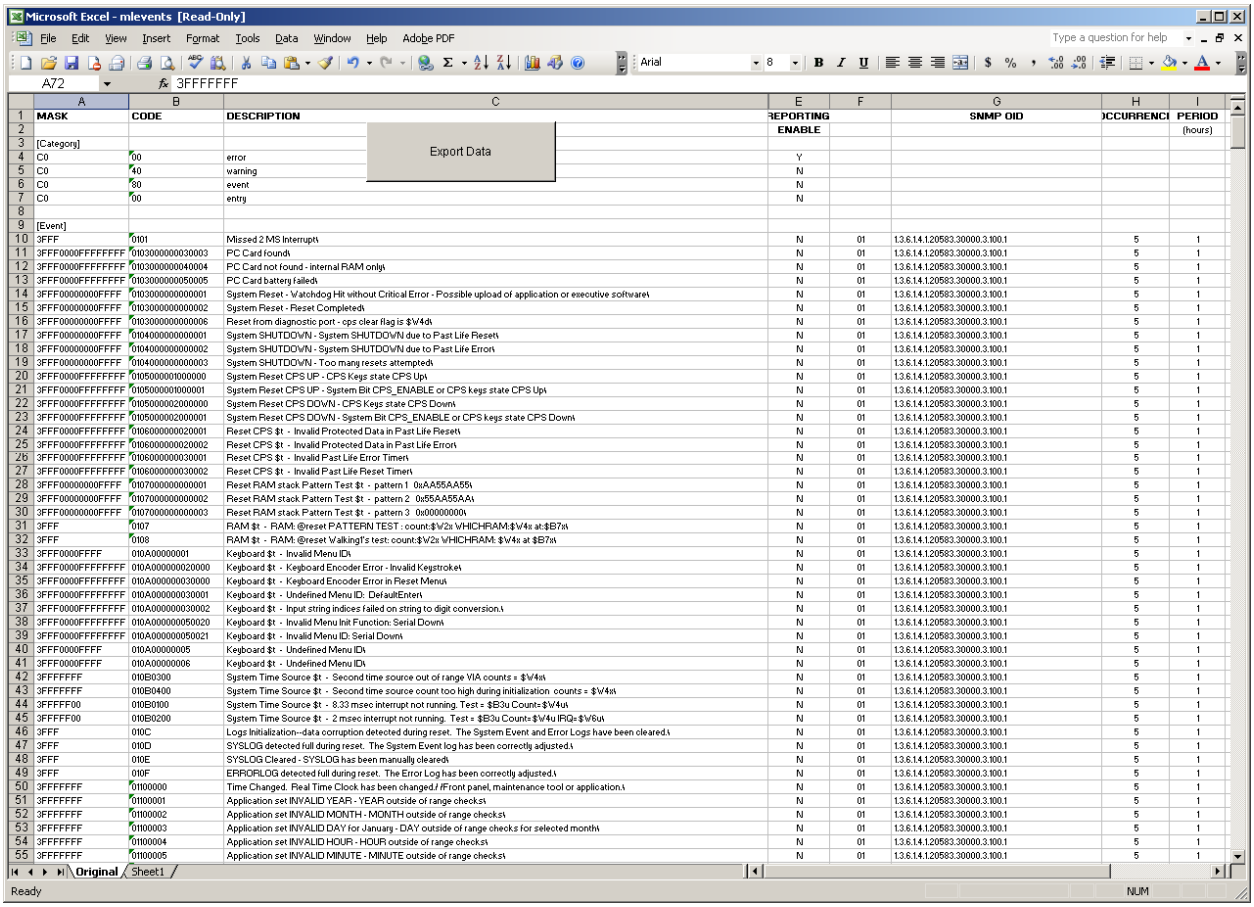
## 4.3. Configuring SNMP Event Traps

### 4.3.1. Generating the MICROLOK II Events File

SMNP Trap/Inform activity is configured using a Microsoft Excel application. This Excel file includes a macro that converts these settings into a text-formatted (.txt) MLK events file. The text file is then placed into the TIM file structure at "home/microlok/mlevents" using WinSCP or similar file transfer utility The name of this file may change, but any change in the file name must be reflected in the configuration servlet.

The MLK events file is generated using a supplied Microsoft Excel spreadsheet (mlevents.xls). The spreadsheet contains a list of every event of interest and the associated code, mask, description, reporting enable ("Y" for yes or "N" for no), SNMP OID, occurrence (number of times the event must occur), and period (time during which the specified number of event occurrences must occur) for each event to be reported.

To generate a MLK Events file from the spreadsheet, the Reporting Enable column should contain a "Y" for each event that will be included in the file. The "Export Data" function can then be selected. A filename will need to be entered (typically this should be "mlevents"). A file (named "mlevents.txt") will then be created on the local file system. The file can then be transferred to the unit and placed in the directory specified above.




| | A | B | C | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|
| 1 | MASK | CODE | DESCRIPTION | REPORTING ENABLE | | SNMP OID | OCCURRENCE | PERIOD (hours) |
| 2 | | | | | | | | |
| 3 | [Category] | | | | | | | |
| 4 | C0 | 00 | error | Y | | | | |
| 5 | C0 | 40 | warning | N | | | | |
| 6 | C0 | 80 | event | N | | | | |
| 7 | C0 | 00 | entry | N | | | | |
| 8 | | | | | | | | |
| 9 | [Event] | | | | | | | |
| 10 | 3FFF | 0101 | Missed 2 MS Interrupt\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 11 | 3FFF0000FFFFFFFF | 0103000000030003 | PC Card found\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 12 | 3FFF0000FFFFFFFF | 0103000000040004 | PC Card not found - internal RAM only\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 13 | 3FFF0000FFFFFFFF | 0103000000050005 | PC Card battery failed\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 14 | 3FFF00000000FFFF | 0103000000000001 | System Reset - Watchdog Hit without Critical Error - Possible upload of application or executive software\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 15 | 3FFF00000000FFFF | 0103000000000002 | System Reset - Reset Completed\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 16 | 3FFF00000000FFFF | 0103000000000006 | Reset from diagnostic port - cps clear flag is $V4d\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 17 | 3FFF00000000FFFF | 0104000000000001 | System SHUTDOWN - System SHUTDOWN due to Past Life Reset\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 18 | 3FFF00000000FFFF | 0104000000000002 | System SHUTDOWN - System SHUTDOWN due to Past Life Error\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 19 | 3FFF00000000FFFF | 0104000000000003 | System SHUTDOWN - Too many resets attempted\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 20 | 3FFF0000FFFFFFFF | 0105000001000000 | System Reset CPS UP - CPS Keys state CPS Up\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 21 | 3FFF0000FFFFFFFF | 0105000001000001 | System Reset CPS UP - System Bit CPS_ENABLE or CPS keys state CPS Up\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 22 | 3FFF0000FFFFFFFF | 0105000002000000 | System Reset CPS DOWN - CPS Keys state CPS Down\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 23 | 3FFF0000FFFFFFFF | 0105000002000001 | System Reset CPS DOWN - System Bit CPS_ENABLE or CPS keys state CPS Down\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 24 | 3FFF0000FFFFFFFF | 0106000000020001 | Reset CPS $t - Invalid Protected Data in Past Life Reset\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 25 | 3FFF0000FFFFFFFF | 0106000000020002 | Reset CPS $t - Invalid Protected Data in Past Life Error\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 26 | 3FFF0000FFFFFFFF | 0106000000030001 | Reset CPS $t - Invalid Past Life Error Timer\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 27 | 3FFF0000FFFFFFFF | 0106000000030002 | Reset CPS $t - Invalid Past Life Reset Timer\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 28 | 3FFF00000000FFFF | 0107000000000001 | Reset RAM stack Pattern Test $t - pattern 1 0xAA55AA55\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 29 | 3FFF00000000FFFF | 0107000000000002 | Reset RAM stack Pattern Test $t - pattern 2 0x55AA55AA\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 30 | 3FFF00000000FFFF | 0107000000000003 | Reset RAM stack Pattern Test $t - pattern 3 0x00000000\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 31 | 3FFF | 0107 | RAM $t - RAM: @reset PATTERN TEST : count:$V2x WHICHRAM:$V4x at:$B7x\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 32 | 3FFF | 0108 | RAM $t - RAM: @reset WalkingI's test: count:$V2x WHICHRAM: $V4x at $B7x\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 33 | 3FFF0000FFFF | 010A00000001 | Keyboard $t - Invalid Menu ID\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 34 | 3FFF0000FFFFFFFF | 010A000000020000 | Keyboard $t - Keyboard Encoder Error - Invalid Keystroke\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 35 | 3FFF0000FFFFFFFF | 010A000000030000 | Keyboard $t - Keyboard Encoder Error in Reset Menu\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 36 | 3FFF0000FFFFFFFF | 010A000000030001 | Keyboard $t - Undefined Menu ID: DefaultEnter\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 37 | 3FFF0000FFFFFFFF | 010A000000030002 | Keyboard $t - Input string indices failed on string to digit conversion.\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 38 | 3FFF0000FFFFFFFF | 010A000000050020 | Keyboard $t - Invalid Menu Init Function: Serial Down\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 39 | 3FFF0000FFFFFFFF | 010A000000050021 | Keyboard $t - Invalid Menu ID: Serial Down\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 40 | 3FFF0000FFFF | 010A00000005 | Keyboard $t - Undefined Menu ID\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 41 | 3FFF0000FFFF | 010A00000006 | Keyboard $t - Undefined Menu ID\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 42 | 3FFFFFFF | 010B0300 | System Time Source $t - Second time source out of range VIA counts = $V4x\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 43 | 3FFFFFFF | 010B0400 | System Time Source $t - Second time source count too high during initialization counts = $V4x\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 44 | 3FFFFF00 | 010B0100 | System Time Source $t - 8.33 msec interrupt not running. Test = $B3u Count=$V4x\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 45 | 3FFFFF00 | 010B0200 | System Time Source $t - 2 msec interrupt not running. Test = $B3u Count=$V4x IRQs=$V6x\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 46 | 3FFF | 010C | Logz Initialization--data corruption detected during reset. The System Event and Error Logs have been cleared.\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 47 | 3FFF | 010D | SYSLOG detected full during reset. The System Event log has been correctly adjusted.\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 48 | 3FFF | 010E | SYSLOG Cleared - SYSLOG has been manually cleared\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 49 | 3FFF | 010F | ERRORLOG detected full during reset. The Error Log has been correctly adjusted.\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 50 | 3FFFFFFF | 01100000 | Time Changed. Real Time Clock has been changed.// /Front panel, maintenance tool or application.\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 51 | 3FFFFFFF | 01100001 | Application set INVALID YEAR - YEAR outside of range checks\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 52 | 3FFFFFFF | 01100002 | Application set INVALID MONTH - MONTH outside of range checks\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 53 | 3FFFFFFF | 01100003 | Application set INVALID DAY for January - DAY outside of range checks for selected month\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 54 | 3FFFFFFF | 01100004 | Application set INVALID HOUR - HOUR outside of range checks\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |
| 55 | 3FFFFFFF | 01100005 | Application set INVALID MINUTE - MINUTE outside of range checks\ | N | 01 | 1.3.6.1.4.1.20583.30000.3.100.1 | 5 | 1 |

**Figure 4-9. Typical mlevents.xls File**

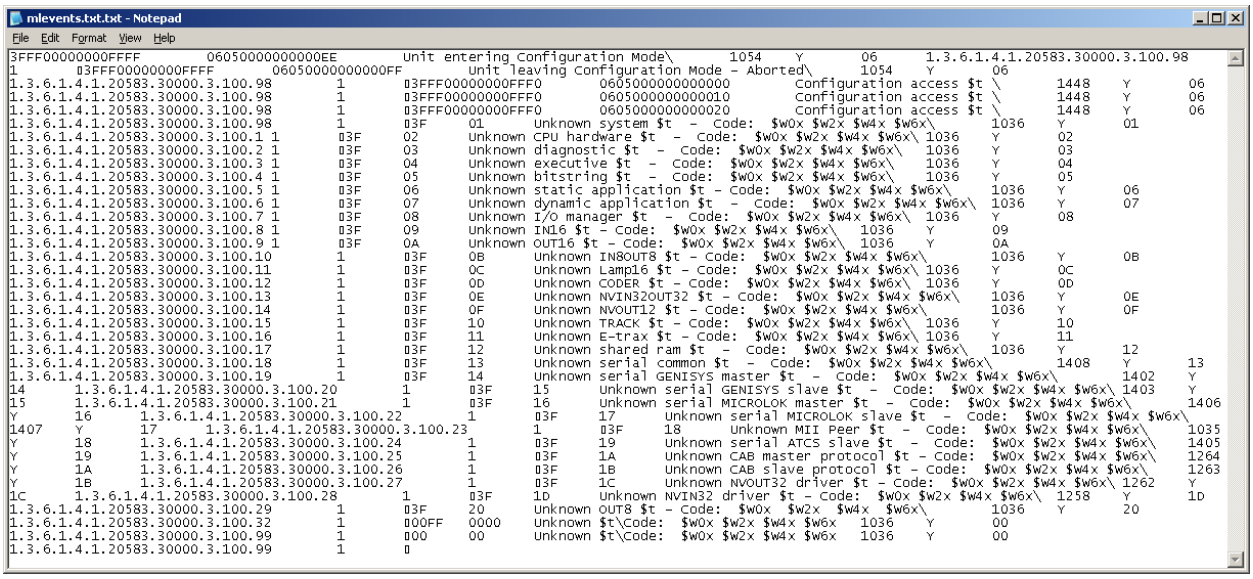



**Figure 4-10. Typical mlevents.txt File**

## 4.3.2. Transferring the mlevents.txt File to the TransPortal Interface Monitor

The mlevents.txt file can be transferred to the TIM using either a Windows computer or a Linux computer.

### 4.3.2.1. Using a Windows-Based Computer

For a windows-based computer, the simplest way to transfer the file to the TIM by using WinSCP (a free program available at http://winscp.net) as follows.

1. From a computer on the same network as the TIM, install WinSCP (if required).
2. Run WinSCP and select create a new connection using the settings listed below. See Figure 4-11 for typical login screen.
   - Host Name: IP address of the TIM on the network
   - Port Number: 22
   - User Name: root
   - Password: arcom
   - Private Key File: (leave blank)
   - File Protocol: SFTP
   - Allow SCP Fallback: Yes

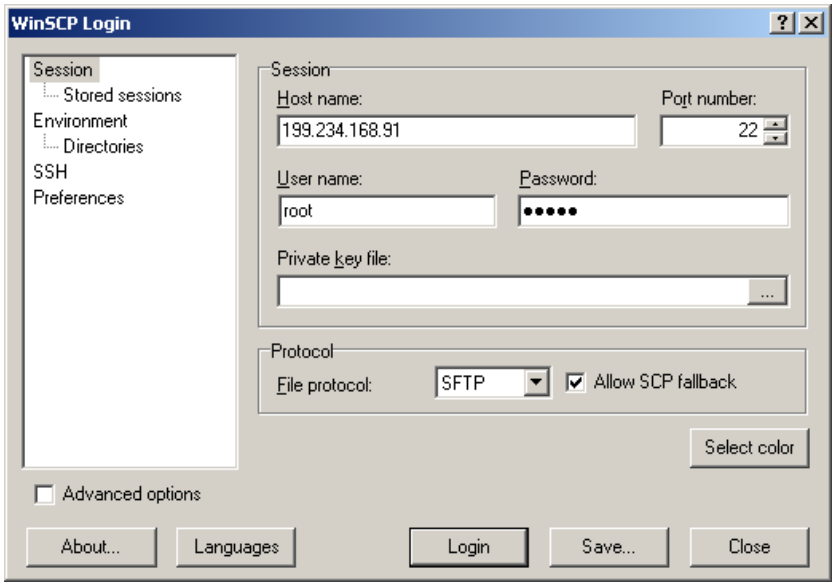



**Figure 4-11. Typical mlevents.txt File Transfer Login (Windows Computer)**

3. After WinSCP has logged into the TIM, the screen will be split into two. See Figure 4-12 for a typical split-screen display.

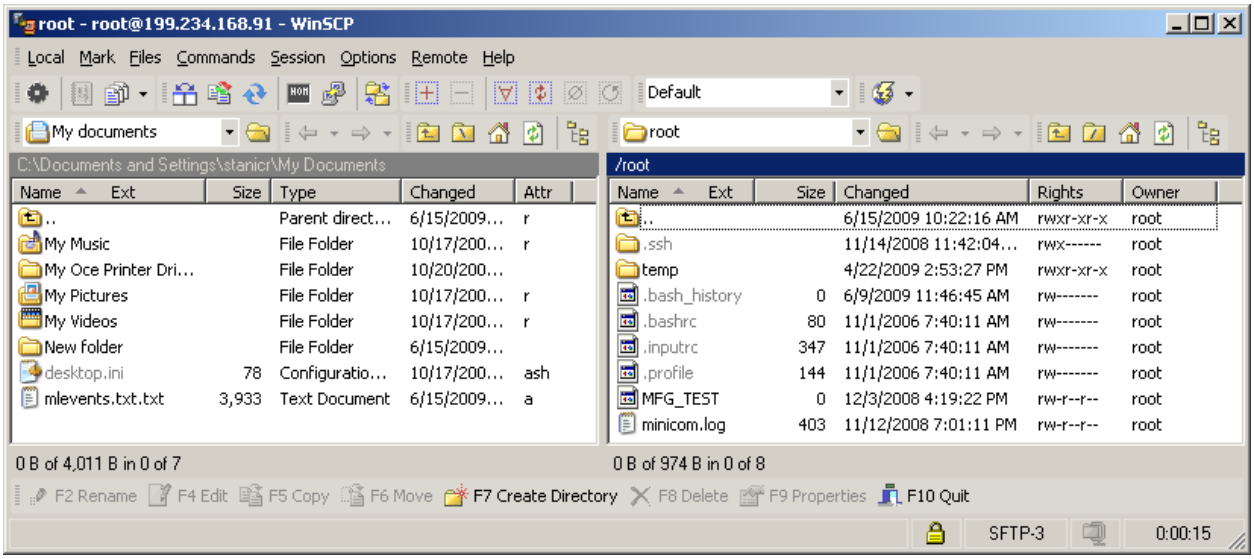

root - root@199.234.168.91 - WinSCP
Local Mark Files Commands Session Options Remote Help
Default
My documents
root
C:\Documents and Settings\stanicr\My Documents
/root
Name Ext Size Type Changed Attr
Name Ext Size Changed Rights Owner
0 B of 4,011 B in 0 of 7
0 B of 974 B in 0 of 8
F2 Rename F4 Edit F5 Copy F6 Move F7 Create Directory F8 Delete F9 Properties F10 Quit
SFTP-3
0:00:15

**Figure 4-12. Typical WinSCP Split Screen (Windows Computer)**

4. Browse to the directory containing the new “mlevents.txt” file on the left, and “<root>/home/microlok” directory on the right. See Figure 4-13 for a typical screen display.

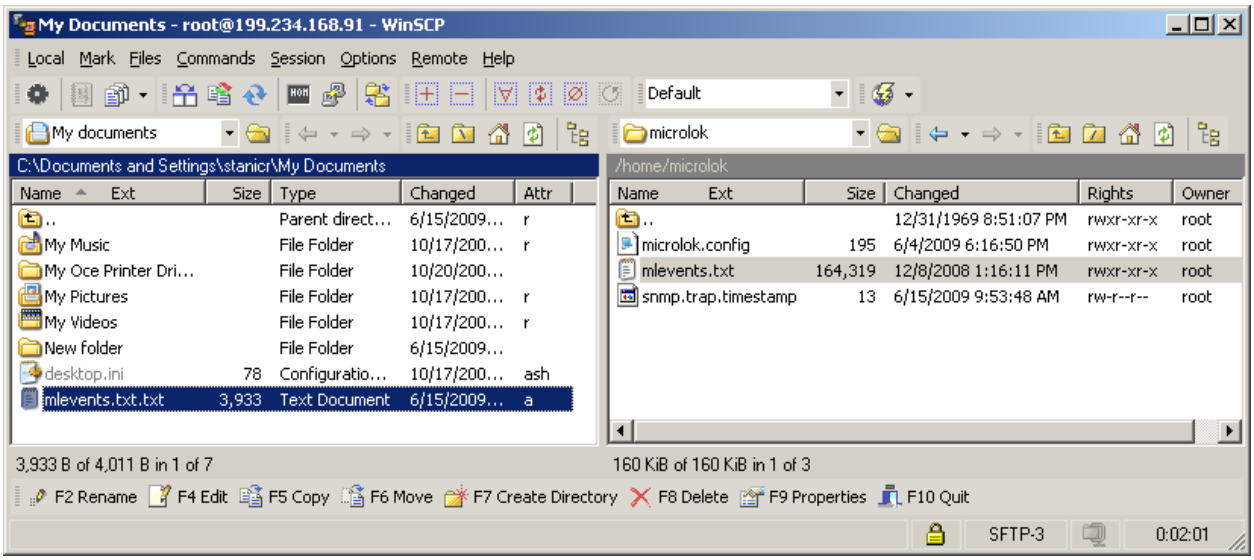

My Documents - root@199.234.168.91 - WinSCP
Local Mark Files Commands Session Options Remote Help
Default
My documents
microlok
C:\Documents and Settings\stanicr\My Documents
/home/microlok
Name Ext Size Type Changed Attr
.. Parent direct... 6/15/2009... r
My Music File Folder 10/17/200... r
My Oce Printer Dri... File Folder 10/20/200...
My Pictures File Folder 10/17/200... r
My Videos File Folder 10/17/200... r
New folder File Folder 6/15/2009...
desktop.ini 78 Configuratio... 10/17/200... ash
mlevents.txt.txt 3,933 Text Document 6/15/2009... a
Name Ext Size Changed Rights Owner
.. 12/31/1969 8:51:07 PM rwxr-xr-x root
microlok.config 195 6/4/2009 6:16:50 PM rwxr-xr-x root
mlevents.txt 164,319 12/8/2008 1:16:11 PM rwxr-xr-x root
snmp.trap.timestamp 13 6/15/2009 9:53:48 AM rw-r--r-- root
3,933 B of 4,011 B in 1 of 7
160 KiB of 160 KiB in 1 of 3
F2 Rename F4 Edit F5 Copy F6 Move F7 Create Directory F8 Delete F9 Properties F10 Quit
SFTP-3
0:02:01

**Figure 4-13. Typical mlevents.txt File Transfer (Windows Computer)**

5. Drag the new “mlevents.txt” file to the right (TIM) window. This overwrites the existing mlevents.txt file in the TIM.
6. Close WinSCP.
7. Reboot the TIM to apply the changes.

#### 4.3.2.2. Using a Linux Computer

For a Linux-based computer, transfer the mlevents.txt file to the TIM as follows:

1. From a computer on the same network as the TIM unit:
   - Run “scp <source> <destination>” from the command line where:

     <source> = full path to the new “mlevents.txt” file
     <destination> = full path (including “root@ip_address”) to the TIM directory
   - For example:

     If the new “mlevents.txt” file is in the “/tmp” directory on the local computer and the IP address of the TIM is 192.169.1.2, enter the following text in the command line:

     “scp /tmp/mlevents.txt root@192.168.1.2/home/microlok/mlevents.txt”

### 4.3.3. SNMP Trap Timestamp File

To prevent the resending of traps/informs upon a system restart, a timestamp of the last trap/inform is stored locally on the unit. The "/home/microlok/snmp.trap.timestamp" file contains this timestamp. When the software starts, this timestamp is read and used to prevent any previously generated traps from being sent to the SNMP manager. The timestamp is updated each time a new trap or inform is sent.

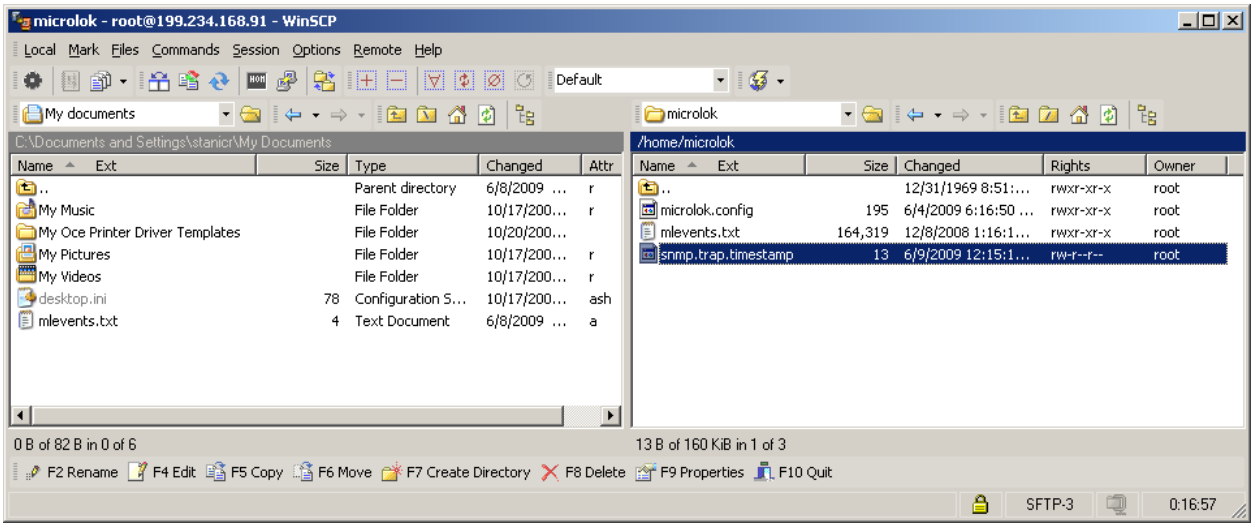

microlok - root@199.234.168.91 - WinSCP
Local Mark Files Commands Session Options Remote Help
Default
My documents
microlok
C:\Documents and Settings\stanicr\My Documents
/home/microlok
Name Ext Size Type Changed Attr
.. Parent directory 6/8/2009 ... r
My Music File Folder 10/17/200... r
My Oce Printer Driver Templates File Folder 10/20/200...
My Pictures File Folder 10/17/200... r
My Videos File Folder 10/17/200... r
desktop.ini 78 Configuration S... 10/17/200... ash
mlevents.txt 4 Text Document 6/8/2009 ... a
Name Ext Size Changed Rights Owner
.. 12/31/1969 8:51:... rwxr-xr-x root
microlok.config 195 6/4/2009 6:16:50 ... rwxr-xr-x root
mlevents.txt 164,319 12/8/2008 1:16:1... rwxr-xr-x root
snmp.trap.timestamp 13 6/9/2009 12:15:1... rw-r--r-- root
0 B of 82 B in 0 of 6
13 B of 160 KiB in 1 of 3
F2 Rename F4 Edit F5 Copy F6 Move F7 Create Directory F8 Delete F9 Properties F10 Quit
SFTP-3
0:16:57

**Figure 4-14. Typical snmp.trap.timestamp File Location**

## 4.4. Invoking the MICROLOK II Development System

The MLK Development System (also referred to as "Dev Tool") is a software application used to communicate with installed MLK systems. This manual covers accessing the "Dev Tool" locally (using a Windows-based computer; typically connected to port ETH0 on the TIM) or remotely (using a network workstation; typically connected to port ETH1 on the TIM). This manual does not cover detailed use of features typically available within the "Dev Tool."

### 4.4.1. Locally at the TransPortal Interlock Monitor

A communication port on the local computer must be configured to interface with Ethernet port ETH0 (typically) on the TIM. This is done using a serial-to-TCP/IP converter application (TCP-Com) included in the "Dev Tool" installation package for this TIM application.

#### 4.4.1.1. Configuring the Local Computer

**NOTE**

The data shown in these web page views are only ***representative*** of the configuration data required for a specific interlocking. Each TIM must be configured with ***interlocking-specific data*** for that location.

Each TIM must also be configured with ***specific*** network- and SNMP-host interface parameters for that location.

1. Access the "Local Area Connection Properties" window on the computer being used. Select "Internet Protocol (TCP/IP)." See Figure 4-15.

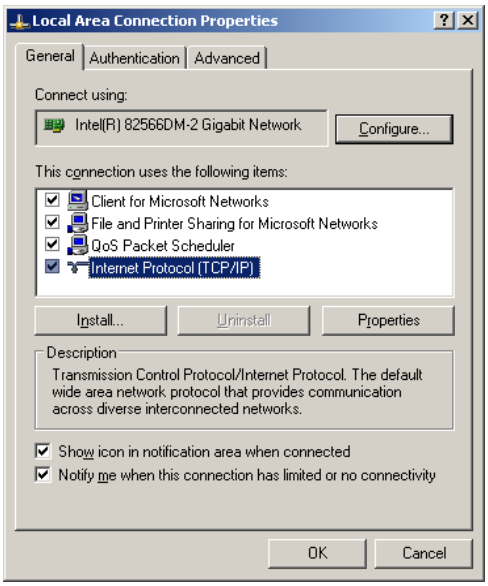



**Figure 4-15. Typical Local Area Connection Properties**

2. Select “Properties,” enter the IP address data for Ethernet port ETH0 (typical) on the TIM, and select “OK.” See Figure 4-16. The IP address data shown is typical; enter the specific data for this TIM application.

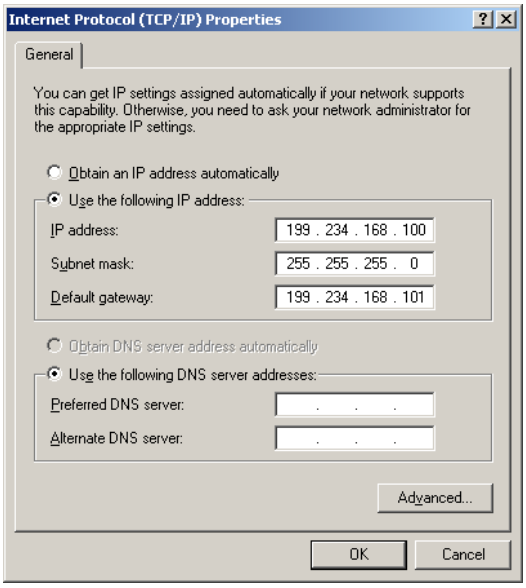

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
199 . 234 . 168 . 100
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
199 . 234 . 168 . 101
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

**Figure 4-16. Typical Local Area Connection Properties (General)**

3. Open the “Authentication” tab and ***deselect*** “Enable IEEE 802.x authentication for this network.” See Figure 4-17.

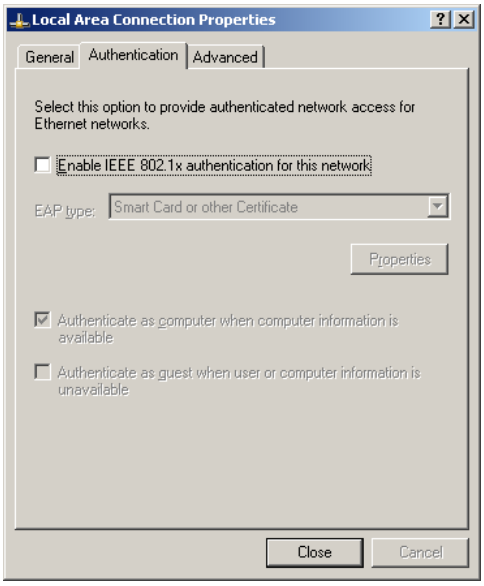

Local Area Connection Properties
General
Authentication
Advanced
Select this option to provide authenticated network access for Ethernet networks.
Enable IEEE 802.1x authentication for this network
EAP type:
Smart Card or other Certificate
Properties
Authenticate as computer when computer information is available
Authenticate as guest when user or computer information is unavailable
Close
Cancel

**Figure 4-17. Typical Local Area Connection Properties (Authentication)**

4. Configure the converter, typically as shown in Figure 4-18 and Figure 4-19. The IP address data shown is typical; enter the specific data for this TIM application.

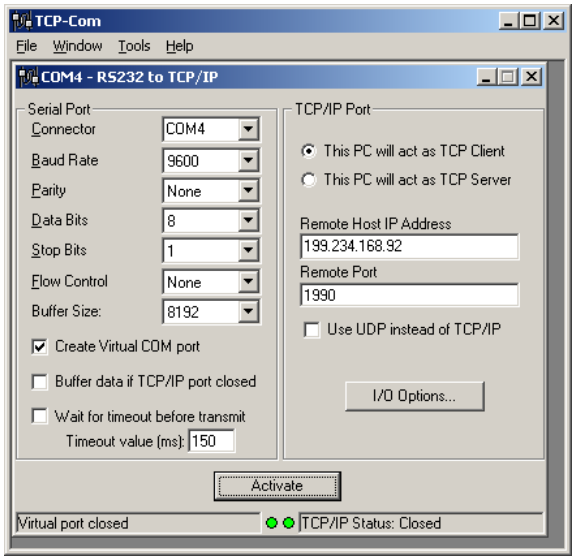



**Figure 4-18. Typical Serial-to-TCP/IP Converter Configuration**

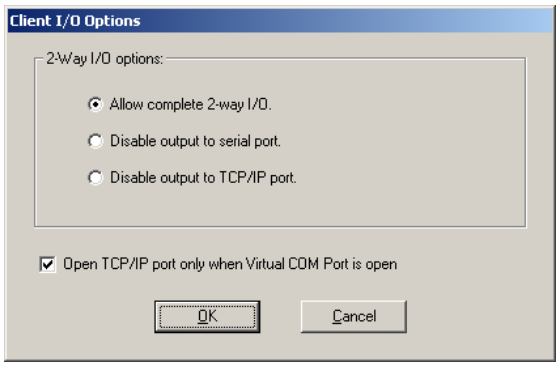

Client I/O Options
2-Way I/O options:
Allow complete 2-way I/O.
Disable output to serial port.
Disable output to TCP/IP port.
Open TCP/IP port only when Virtual COM Port is open
OK
Cancel

**Figure 4-19. Typical Serial-to-TCP/IP Converter I/O Options Configuration**

### 4.4.1.2. Running the MICROLOK II Development System

All features of the MLK Development System (also referred to as "Dev Tool") for this TIM application are now available. To access the "Dev Tool", proceed as follows.

1. Connect the computer to Ethernet port ETH0 (typical) on the TIM. If required, configure the computer for this TIM application (Refer to Section 4.4.1.1).

2. Open TCP-Com (See Figure 4-18.) and select “Activate.” See Figure 4-20.

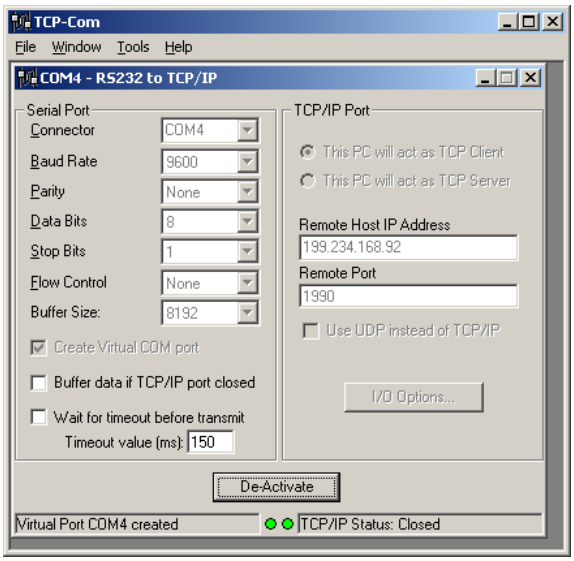



**Figure 4-20. Typical Serial-to-TCP/IP Converter (Activated)**

3. Launch the “Dev Tool” on the computer desktop. The communications pop-up will appear. See Figure 4-21.

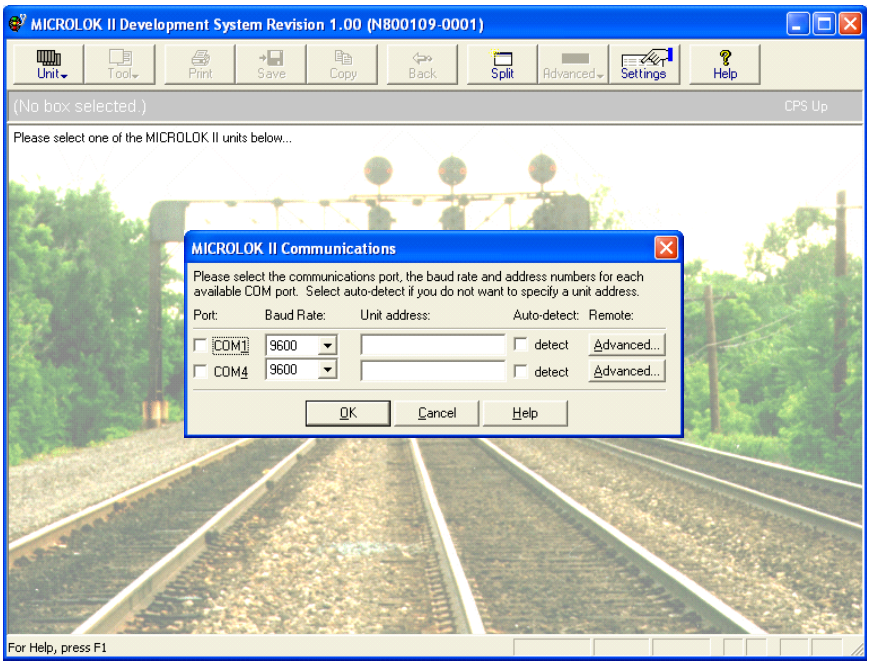



**Figure 4-21. Typical MICROLOK II Development System Communications Pop-up**

4. Select the communication port activated in TCP-Com and enter the IP address of the Ethernet port (ETH0 typical) as the "Unit address." See Figure 4-22. The address data shown is typical; enter the specific data for this TIM application.

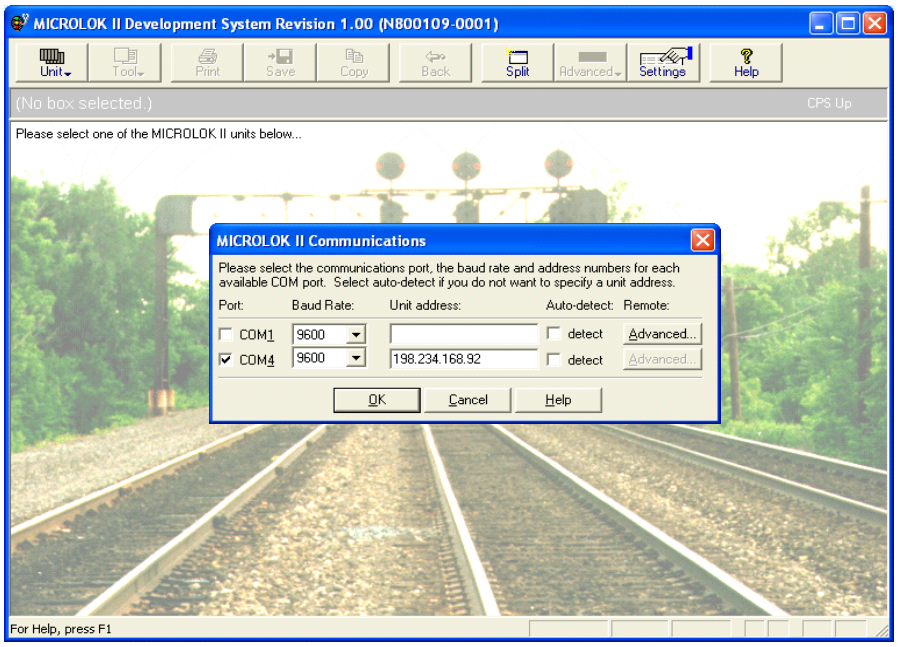



**Figure 4-22. Typical MICROLOK II Development System Communications Setup**

5. Select "OK." The "Dev Tool" will show the available MLK unit(s). See Figure 4-23

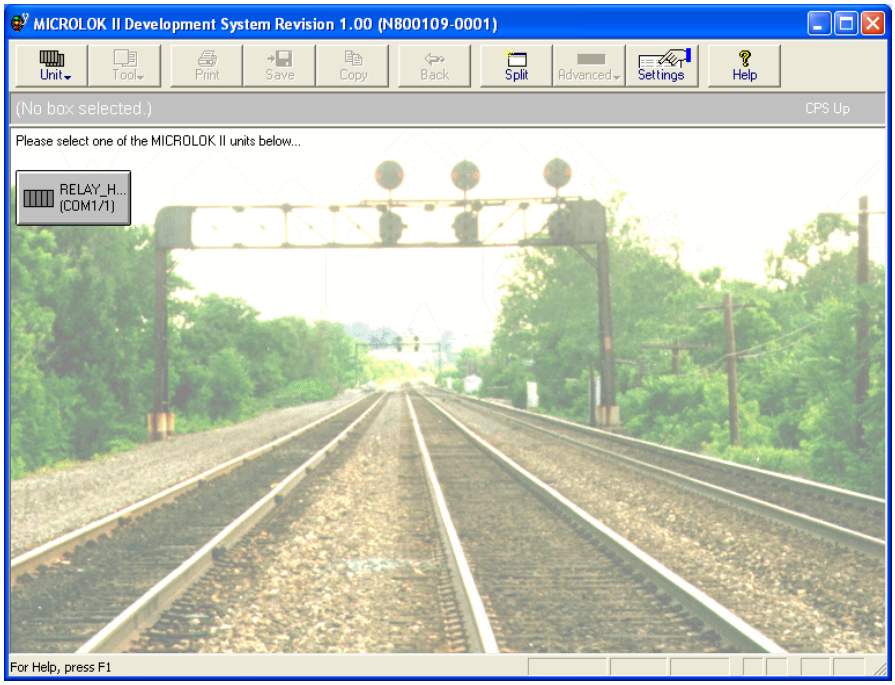



**Figure 4-23. Typical MICROLOK II Development System Site Display**

6. Select the desired MLK unit to display the Main Menu for the unit. See Figure 4-24.

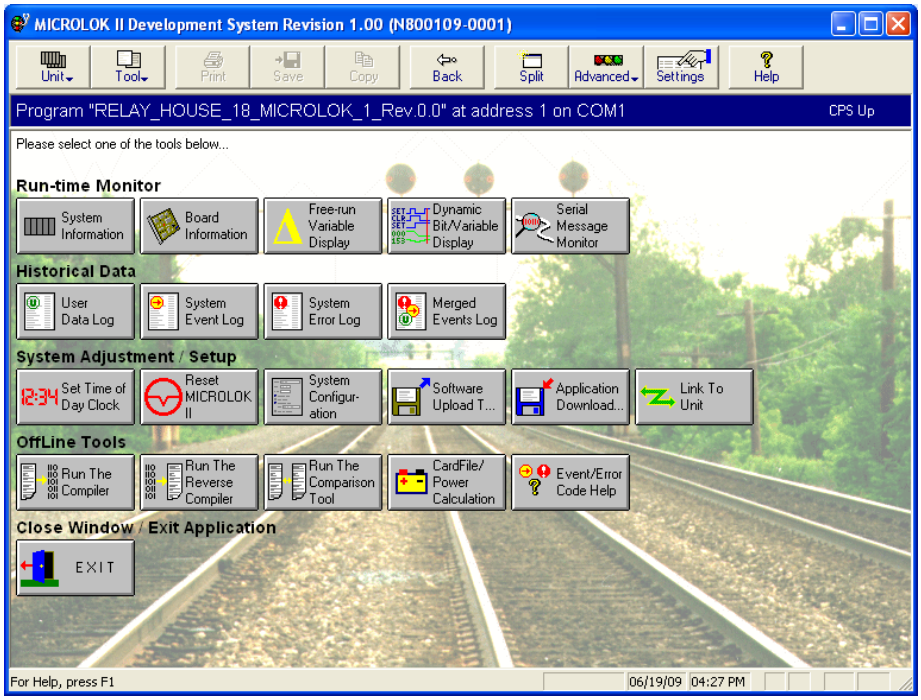



**Figure 4-24. Typical MICROLOK II Development System Main Menu**

### 4.4.2. Remotely from a Computer Network Workstation

The MICROLOK II (MLK) Development System ("Dev Tool") must be loaded onto the workstation being used. TCP-Com must also be loaded and configured to communicate with the MLK (Refer to Section 4.4.1.1).

1. Navigate to the NimBUS dashboard (or similar server application showing installed MLK systems) using Internet Explorer.
2. Right-click on the MLK system of interest and select "Dev Tools" from the popup menu. See Figure 4-25.
3. If the "Dev Tool" is installed on the workstation and TCP-Com is configured properly and activated, "Dev Tools" will launch automatically, connect to the selected MLK system, and display the "Dev Tool" main menu. If not, verify that TCP-Com is installed, configured properly for this application, and activated.

**Figure 4-25. Typical Network Dashboard Screen**

# 5. SUPPORT AND MAINTENANCE

There are no user serviceable parts or components in the TransPortal Interlock Monitor (TIM).

The unit is shipped with an internal lithium battery enabled, supporting the unit's real time clock. While the battery-backed clock provides for faster unit startup, it is entirely optional for proper operation because the TIM has several means of obtaining the proper date and time for operation (i.e., over the network and using GPS, if so equipped). The battery has a predicted lifetime of greater than seven years. If, in the future, the battery is exhausted, its replacement is optional.

The Rapid Action Information Link Team (RAIL Team) is a group of experienced product and application engineers ready to assist you to resolve any technical issues concerning this product. Contact the RAIL Team in the United States at 1-800-652-7276 or by e-mail at railteam@ansaldo-sts.us.

It is helpful to have the following information at hand when calling to expedite support and gaining prompt assistance:

- The TIM serial number, located on the side of the device adjacent to the barcode pattern.
- The model number of the device.
- Knowledge of the network connection scheme used for the installation – cellular radio, private wired network, or private wireless network.

# 6. GLOSSARY, ABBREVIATIONS, AND ACRONYMS

The following terms, abbreviations, and acronyms used in this manual.

| | |
|---|---|
| 10/100Base-T | The physical connection layer used by TCP/IP and typically implemented in a Category 5 cable. |
| AAR | American Association of Railroads |
| AREMA | American Railway Engineering and Maintenance-of-Way Association, a North American railway industry group. |
| CAT5 | Category 5 cable, unshielded twisted pair type cable, a standard networking cable terminated with an RJ-45 compatible plug. |
| CDMA | Code Division Multiple Access, a cellular channel methodology, contrasted with GSM. |
| CLASS C EQUIPMENT | AREMA classification of the TransPortal device, used in protective bungalows or similarly NEMA-rated enclosures. |
| CPU | Central Processing Unit, also microprocessor. |
| DHCP | Dynamic Host Configuration Protocol, a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual intervention. |
| DNS | Domain Name System, a hierarchical naming system for computers and networked connected devices, translates readable addresses to their respective routable numeric addresses. |
| DOT (NUMBER) | Department of Transportation, a unique physical asset identification number used in the US transportation industry. |
| EMI | Electromagnetic Interference, radiated emissions from a device that can disrupt operation of an adjacent device. |
| ESN | Electronic Serial Number, a unique identifier for a cellular radio device. |
| FCC | Federal Communications Commission |
| FQDN | Fully Qualified Domain Name |
| FRA | Federal Railway Administration, the railroad sector of the US Department of Transportation. |
| FTP | File Transfer Protocol, a networking protocol for transferring data files. |
| GPS | Global Positioning System, world-wide latitude and longitudinal position determination network which also provides accurate synchronized time of day. |

| | |
|---|---|
| GSM | Global System for Mobile communications: originally from Groupe Spécial Mobile) is a global form of cellular communications, contrasted with CDMA. |
| HMAC | Hash-keyed Message Authentication Code, a complex data packet used to implement data encryption and security. |
| IMSI | International Mobile Subscriber Identity, a unique number associated with all GSM, CDMA, and UMTS network mobile devices. |
| IO or I/O | Input/Output points. |
| IP | Internet Protocol, a networking term implying the use of standard TCP/IP networking protocol. |
| LAN | Local Area Network |
| LCD | Liquid Crystal Display |
| LED | Light Emitting Diode |
| LOD | Lamp Outage Detector, an electronic warning lamp circuit monitor manufactured by General Electric transportation Systems (fka Harmon). |
| MAC | Media Access Controller, a globally unique address of a networking port, typically associated with an RJ-45 jack. |
| MD5 CHECKSUM | Message-Digest algorithm 5 is a widely used cryptographic hash function with a 128-bit hash value data validation parameter that guarantees the authenticity of data, in this case used by the TransPortal event recorder to authenticate event data records. |
| MIN | Mobile ID Number, the unique cellular address of a CDMA or GSM connected device. |
| NAT | Network Address Translation, the process of modifying network address information in datagram packet headers while in transit across a traffic routing device for the purpose of remapping a given address space into another. |
| NEMA | National Equipment Manufacturers Association, provides a standard rating system for characterizing the environmental qualifications of outdoor equipment and enclosures . |
| PIO | Physical I/O (input/output), the TransPortal service that correlates physical I/O connections to TransPortal RNAMES. |
| RNAME | Reserved Name, the label of a data field used by the TransPortal to evaluate monitored points within alarm determination services. |
| RS-232 | Common serial communication protocol. |
| RSSI | Received Signal Strength Indicator, a metric used to quantify cellular signal strength and quality, ranging between –60dB (strong) and –100dB (weak). |

| | |
|---|---|
| SD FLASH | Secure Digital Flash (Memory), a non-volatile, non-battery backed solid state memory device used by the TransPortal for event recording. |
| SERVLET | A Java application that runs in a Web server or application server and provides server-side processing such as accessing a database and e-commerce transactions. |
| SID | System ID, the unique address or identity of a cellular system. |
| SNMP | Simple Network management Protocol, a networking protocol typically used to manage the operation of networked printers and routers. |
| TCP/IP | Standard networking and internetworking protocol |
| UDP | User Datagram Protocol, a non-standard or proprietary networking protocol alternative to standardized TCP/IP. |
| UMTS | Universal Mobile Telecommunications System |
| USB | Universal Serial Bus, high speed serial bus standard to connect devices to a host computer. |
| VDC | Volts Direct Current |
| WAN | Wide Area Network |
| VPN | Virtual Private Network, a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) as opposed to running across a single private network. |

**End of Manual**